Indiana License Plate and Registration Fulfillment Security Plan

Table of Contents

Purpose

The purpose of this document it to serve as the Security Plan for the production and distribution of License plates and Registration documents for the Indiana Bureau of Motor Vehicles (BMV). The Security Plan is an overview of systems, processes, policies, and controls that are designed to ensure that the confidentiality, integrity, and availability of Indiana BMV information is maintained throughout the life of the contract. The controls outlined in this document are in-line with the *SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations (Final Public Draft)* published in March 2020. This is a living document and will be updated in parallel with changes made to the IHGIN and BIS Information Security Policies on an annual basis.

Scope

The Indiana License Plate and Registration Fulfillment Security Plan will highlight the technical and process related controls put in place to help safeguard the information provided to IHGIN by the BMV and third-party contractors. This document will take a full picture view of security operations considering the 8 domains of systems security as outlined by ISC^2 and the different security controls that can be utilized to enforce compliance through both technical and non-technical means.

Security Controls

IHGIN and BIS maintain strict IT security standards and controls. IHGIN takes steps to ensure that customer data is controlled and maintained in a manner that ensures the confidentiality, integrity, and availability of Indiana information and data. The controls below highlight sections of the *SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations (Final Public Draft)* published in March 2020. Additional controls have been implemented to help safeguard non-IT assets to ensure that information, materials, and data remain protected through end of life.

Access Control

Control ID	**AC-1**	Control Name	**Policy and Procedures**
Definition	a. Develop, document, and disseminate to personnel: a) [Selection (one or more): organization-level; mission/business process-level; system-level] access control policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and b) Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency]; and		

	2. Procedures [Assignment: organization-defined frequency]
IHGIN Response	To assure compliance with control AC-1, IHGIN maintains an access control policy within the organizational IT security policy that is a requirement of staff to adhere to. The IT security policy meets the directives of this control and is managed by William MacDonald the IT Architect for IHGIN. It is reviewed on a semi-annual basis or at any-time that there is major technological change within the IHGIN IT systems.

Control ID	**AC-2**	Control Name	**Account Management**
Definition	a. Define and document the types of accounts allowed for use within the system; b. Assign account managers; c. Establish conditions for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, and conditions]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time-period] when accounts are no longer required; 2. [Assignment: organization-defined time-period] when users are terminated or transferred; and 3. [Assignment: organization-defined time-period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and 3. [Assignment: organization-defined attributes (as required)]; j. Review accounts for compliance with account management requirements [Assignment: organization-defined frequency]; k. Establish and implement a process for changing shared or group account credentials (deployed) when individuals are removed from the group; and l. Align account management processes with personnel termination and transfer processes		
IHGIN Response	The IHGIN IT Security policy establishes the requirements that ensure that account access and management is signed off on by an employee's immediate supervisor. IT retains the right to deny account access at any time without notice or reason to staff.		

	Access requirements are reviewed on a quarterly basis and continued access requires managerial approval. When a staff member is dismissed or leaves the organization IT is to be made aware and will immediately de-activate any accounts and access the user may have had in addition to seizing any IT assets the employee may have used. Whenever systems access is required or changed, IT requires notice from the staff member's manager prior to giving any access to systems or information.

Control ID	**AC-2(1)**	Control Name	**AUTOMATED SYSTEM ACCOUNT MANAGEMENT**
Definition	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	IT systems will notify account managers via email automatically when user access is changed or transferred. All account activity is audited and baselined using a security information and event management solution, any non a-typical user behavior will prompt IT to investigate.		

Control ID	**AC-2(2)**	Control Name	**AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT**
Definition	Automatically [Selection: remove; disable] temporary and emergency accounts after [Assignment: organization-defined time-period for each type of account].		
IHGIN Response	Temporary access to systems expire after a 30 day time period. Any documents internally shared outside of the organization are controlled by access control lists and expire automatically after a 30 day time period.		

Control ID	**AC-2(3)**	Control Name	**DISABLE ACCOUNTS**
Definition	Disable accounts when the accounts: a) Have Expired; b) Are no longer associated with a user or individual; c) Are in violation of organizational policy; or d) Have been inactive for [Assignment: organization-defined time-period].		
IHGIN Response	Accounts that have expired or not been active within the past 90 days are disabled. Accounts associated with staff that may be on extended leave are placed into a special user group with limited access until they return. Any accounts no longer associated directly to an individual are handed off to their replacement and access is removed after 90 days. If an account is found to be in violation of the security policy it is immediately disabled.		

Control ID	**AC-2(4)**	Control Name	**AUTOMATED AUDIT ACTIONS**
Definition	Automatically audit account creation, modification, enabling, disabling, and removal actions.		
IHGIN Response	These policies are created and enforced using group policy management and monitored using our security information and event management suite.		

Control ID	**AC-2(5)**	Control Name	**INACTIVITY LOGOUT**
Definition	Require that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out]		
IHGIN Response	Users are automatically logged out of software based systems after 30 minutes of inactivity and will need to reauthenticate. Their systems will automatically lock and require reauthentication after 10 minutes of user inactivity.		

Control ID	**AC-2(6)**	Control Name	**DYNAMIC PRIVILEGE MANAGEMENT**
Definition	Implement [Assignment: organization-defined dynamic privilege management capabilities].		
IHGIN Response	If a user is changed into a new role, their privileges will dynamically change to allocate the privileges associated with that role and remove the privileges associated with the old role. The SIEM solution will lockout accounts that are operating outside of their normal baseline after hours. During operational hours IT will respond to these events in real-time.		

Control ID	**AC-2(7)**	Control Name	**PRIVILEGED USER ACCOUNTS**
Definition	A. Establish and administer privileged user accounts in accordance with [Selection: a role based access scheme; an attribute-based access scheme]; B. Monitor privileged role or attribute assignments; C. Monitor changes to roles or attributes; and D. Revoke access when privileged role or attribute assignments are no longer appropriate.		
IHGIN Response	Privileged accounts are restricted to software and IT users that require access. These accounts are not to be used daily, but instead the run-as function is to be utilized where possible. All accounts are monitored for any privilege or attribute changes using a combination of group policy objects and the SIEM solution. Privileged access is reviewed quarterly and removed whenever no longer needed.		

Control ID	**AC-2(8)**	Control Name	**DYNAMIC ACCOUNT MANAGEMENT**
Definition	Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dynamically		
IHGIN Response	Quarterly reports are generated of all accounts that exist. The manager responsible for each role is to respond on the continued need for access. Account deactivations are a manual human side process, but the creation of accounts and assignment of roles is dynamic in nature. It just requires the human touch to implement access. Access to certain data can be requested by a staff member at any time, and access can be granted directly by their manager without IT intervention. The audit log trail is created and reviewed by IT staff on a regular basis and the SIEM solution will flag any changes that are outside of user norms.		

Control ID	**AC-2(9)**	Control Name	**RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS**
Definition	Only permit the use of shared and group accounts that meet [Assignment: defined conditions for establishing shared and group accounts].		
IHGIN Response			

Control ID	**AC-2(10)**	Control Name	**SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE**
Definition	Deprecated (Incorporated into AC-2K)		
IHGIN Response	See response to AC-2K		

Control ID	**AC-2(11)**	Control Name	**Usage Conditions**
Definition	Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].		
IHGIN Response	The SIEM solution monitors accounts and reports on any access outside of a specific user's normal baseline. To increase accountability, managers have a direct role in ensuring that access is restricted only to what is needed using the principle of least privilege. Privileged system accounts are restricted to IT staff only and the usage is only on a per need basis.		

Control ID	**AC-2(12)**	Control Name	**ACCOUNT MONITORING FOR ATYPICAL USAGE**
Definition	A. Monitor system accounts for [Assignment: organization-defined atypical usage]; and B. Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].		
IHGIN Response	The SIEM solution accomplishes this task. All systems accounts are monitored and any usage of any account that is non-typical is reported to IT and investigated.		

Control ID	**AC-2(13)**	Control Name	**DISABLE ACCOUNTS FOR HIGH-RISK USERS**
Definition	Disable accounts of users within [Assignment: organization-defined time-period] of discovery of [Assignment: organization-defined significant risks]		
IHGIN Response	Any account that is used to access systems outside of the scope of that account or role is immediately suspended and the usage is investigated. All users are treated as high-risk users and their access is monitored and investigated. HR has the power at any time to request to see what an account has been doing in the environment and the account can be suspended or limited at any time without notice.		

Control ID	**AC-2(14)**	Control Name	**PROHIBIT SPECIFIC ACCOUNT TYPES**
Definition	Prohibit the use of [Selection (one or more): shared; guest; anonymous; temporary; emergency] accounts for access to [Assignment: organization-defined information types].		

IHGIN Response	Shared accounts are strictly prohibited within internal systems. For external non-essential systems that may have 1 organizational account, the password is cycled frequently and managed using our password management solution.

Control ID	**AC-3**	Control Name	**Access Enforcement**
Definition	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies		
IHGIN Response	Logical access to systems is approved by the direct manager and handed off to IT for implementation under the guidance of the Information Security Policy.		

Control ID	**AC-3(1)**	Control Name	**RESTRICTED ACCESS TO PRIVILEGED FUNCTION**
Definition	Deprecated (Incorporated into AC-6)		
IHGIN Response	See response to AC-6		

Control ID	**AC-3(2)**	Control Name	**DUAL AUTHORIZATION**
Definition	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].		
IHGIN Response	Authorization for access to systems and information is required by both the direct managerial report, and IT management.		

Control ID	**AC-3(3)**	Control Name	**MANDATORY ACCESS CONTROL**
Definition	Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy, and where the policy: a) Is uniformly enforced across the covered subjects and objects within the system; b) Specifies that a subject that has been granted access to information is constrained from doing any of the following; 1. Passing the information to unauthorized subjects or objects; 2. Granting its privileges to other subjects; 3. Changing one or more security attributes (specified by the policy) on subjects, objects, the system, or system components; 4. Choosing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects; and 5. Changing the rules governing access control; and c) Specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges] such that they are not limited by any defined subset (or all) of the above constraints		
IHGIN Response	Information sharing and document management is outlined the Information Security Policy. The policy is enforced for all staff and limits the passing of information to unauthorized subjects. The policy is enforced through document governance rules that limit the ability of users to fulfill these tasks without authorization.		

Control ID	**AC-3(4)**	Control Name	**DISCRETIONARY ACCESS CONTROL**
Definition	Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy, and where the policy specifies that a subject that has been granted access to information can do one or more of the following: a) Pass the information to any other subjects or objects; b) Grant its privileges to other subjects; c) Change security attributes on subjects, objects, the system, or the system's components; d) Choose the security attributes to be associated with newly created or revised objects; or e) Change the rules governing access control.		
IHGIN Response	We use mandatory access controls that require dual authorization for access to information. For systems that use discretionary access control, the access is audited, and a business need for access to the data and systems is required by the manager. Otherwise access will be revoked.		

Control ID	**AC-3(5)**	Control Name	**SECURITY-RELEVANT INFORMATION**
Definition	Prevent access to [Assignment: organization-defined security-relevant information] except during secure, non-operable system states		
IHGIN Response	Only IT and Executive staff have access to this information. IT has access to the digital copies of this data, and executive staff have access to backups of this data stored off-site for disaster recovery purposes.		

Control ID	**AC-3(6)**	Control Name	**PROTECTION OF USER AND SYSTEM INFORMATION**
Definition	Deprecated (Incorporated into MP-4 and SC-28)		
IHGIN Response	See response to MP-4 & SC-28		

Control ID	**AC-3(7)**	Control Name	**ROLE-BASED ACCESS CONTROL**
Definition	Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles]		
IHGIN Response	For non-sensitive data pertaining to internal operations we use role-based access controls enforced through group policy management. For customer data and information, we use mandatory access controls.		

Control ID	**AC-3(8)**	Control Name	**REVOCATION OF ACCESS AUTHORIZATIONS**
Definition	Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].		
IHGIN Response	Any changes to a user's group membership will automatically change their access to systems and data in-line with the group policy settings associated with their new role.		

Control ID	**AC-3(9)**	Control Name	**CONTROLLED RELEASE**
Definition	Release information outside of the system only if: a) The receiving [Assignment: organization-defined system or system component] provides [Assignment: organization-defined controls]; and b) Assignment: organization-defined controls] are used to validate the appropriateness of the information designated for release.		
IHGIN Response	Information is only handed off between IHG and the clients directly using TLS 1.2 and IPSEC or better. Any data being transmitted to a client is reviewed by customer service staff to determine the appropriateness of the information being transmitted.		

Control ID	**AC-3(10)**	Control Name	**AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS**
Definition	Employ an audited override of automated access control mechanisms under [Assignment: organization-defined conditions] by [Assignment: organization-defined roles].		
IHGIN Response	Override of access control systems can only be implemented by the administrator and all access is logged and audited using a SIEM solution.		

Control ID	**AC-3(11)**	Control Name	**RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES**
Definition	Restrict access to data repositories containing [Assignment: organization-defined information types].		
IHGIN Response	Access is restricted using role based access controls and audited using a SIEM solution.		

Control ID	**AC-3(12)**	Control Name	**ASSERT AND ENFORCE APPLICATION ACCESS**
Definition	A) Require applications to assert, as part of the installation process, the access needed to the following system applications and functions: [Assignment: organization-defined system applications and functions]; B) Provide an enforcement mechanism to prevent unauthorized access; and C) Approve access changes after initial installation of the application		
IHGIN Response	Any applications require IT approval prior to installation and the need for access to any internal systems functions such as location services, camera, keyboard, microphone, network, files, etc. are determined by IT management and controlled through the installation process.		

Control ID	**AC-3(13)**	Control Name	**ATTRIBUTE-BASED ACCESS CONTROL**
Definition	Enforce attribute-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined attributes to assume access permissions].		
IHGIN Response	File attributed can be specified and access controls implemented based upon a combination or file attributes and user roles. Currently IHGIN does not use attribute based access controls, but has the ability to implement this function if required.		

Control ID	**AC-3(14)**	Control Name	**INDIVIDUAL ACCESS**

Definition	Provide [Assignment: organization-defined mechanisms] to enable individuals to have access to the following elements of their personally identifiable information: [Assignment: organization-defined elements].
IHGIN Response	IHGIN does not provide individuals the ability to view their PII within our system to verify the information is correct. Any PII handed over by the client is stored while in use and then removed from systems immediately after use.

Control ID	**AC-3(15)**	Control Name	**DISCRETIONARY AND MANDATORY ACCESS CONTROL**
Definition	A) Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy; and B) Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy.		
IHGIN Response	IHGIN uses a combination of discretionary and mandatory access controls to systems and data.		

Control ID	**AC-4**	Control Name	**Information Flow Enforcement**
Definition	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].		
IHGIN Response	IHGIN maintains strict information flow controls over customer facing systems and systems holding customer data. Access is restricted by IP address and user account. All activity is logged and analyzed to ensure compliance. We do not use data classifications of secret or top secret to control access.		

Control ID	**AC-4(1)**	Control Name	**OBJECT SECURITY AND PRIVACY ATTRIBUTES**
Definition	Use [Assignment: organization-defined security and privacy attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.		
IHGIN Response	This is not applicable as we do not deal with data classifications of secret or top secret.		

Control ID	**AC-4(2)**	Control Name	**PROCESSING DOMAINS**
Definition	Use protected processing domains to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.		
IHGIN Response	IHGIN utilizes processing domains to identify users as being internal to the organization.		

Control ID	**AC-4(3)**	Control Name	**DYNAMIC INFORMATION FLOW CONTROL**
Definition	Enforce [Assignment: organization-defined information flow control policies].		
IHGIN Response	IHGIN utilizes advanced threat intelligence and AI to change information access and access to systems if there is any change in risk tolerance due to emerging threats.		

Control ID	**AC-4(4)**	Control Name	**FLOW CONTROL OF ENCRYPTED INFORMATION**
Definition	Prevent encrypted information from bypassing [Assignment: organization-defined information flow control mechanisms] by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method]].		
IHGIN Response	IHGIN ensures that all sessions between internal systems and any system containing private customer data is encrypted. Access is logged and analyzed in real-time to ensure that encrypted data is not removed from systems.		

Control ID	**AC-4(5)**	Control Name	**EMBEDDED DATA TYPES**
Definition	Enforce [Assignment: organization-defined limitations] on embedding data types within other data types.		
IHGIN Response	IHGIN utilizes an advanced threat analysis to analyze incoming and outgoing data to ensure that there are files are not embedded into other files.		

Control ID	**AC-4(6)**	Control Name	**METADATA**
Definition	Enforce information flow control based on [Assignment: organization-defined metadata].		
IHGIN Response	IHGIN utilizes metadata to tag files and information internally to accurately describe the content types. Currently it is not used to restrict data flow, but this can be implemented if required.		

Control ID	**AC-4(7)**	Control Name	**ONE-WAY FLOW MECHANISMS**
Definition	Enforce one-way information flows through hardware-based flow control mechanisms		
IHGIN Response	IHGIN enforces read-only access on files based upon user need. For file uploads we can ingest files one-way only.		

Control ID	**AC-4(8)**	Control Name	**SECURITY AND PRIVACY POLICY FILTERS**
Definition	A) Enforce information flow control using [Assignment: organization-defined security or privacy policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]; and B) [Selection (one or more): block; strip; modify; quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security or privacy policy].		
IHGIN Response	IHGIN filters outgoing data based upon security and privacy policy filters to ensure that PII is not transferred outside of the organization.		

Control ID	**AC-4(9)**	Control Name	**HUMAN REVIEWS**
Definition	Enforce the use of human reviews for [Assignment: organization-defined information flows] under the following conditions: [Assignment: organization-defined conditions].		
IHGIN Response	IHGIN IT staff review policy filter violations on a regular basis to ensure that it is meeting the required needs of the business.		

Control ID	**AC-4(10)**	Control Name	**ENABLE AND DISABLE SECURITY OR PRIVACY POLICY FILTERS**
Definition	Provide the capability for privileged administrators to enable and disable [Assignment: organization-defined security or privacy policy filters] under the following conditions: [Assignment: organization-defined conditions].		
IHGIN Response	IHGIN administrators can enable or disable security and privacy policy filters on an as-needed basis. This is done with discretion and any changes to these policies are logged.		

Control ID	**AC-4(11)**	Control Name	**CONFIGURATION OF SECURITY OR PRIVACY POLICY FILTERS**
Definition	Provide the capability for privileged administrators to configure [Assignment: organization-defined security or privacy policy filters] to support different security or privacy policies		
IHGIN Response	IHGIN administrators can change the configuration or create new security and privacy policies based upon business and compliance requirements.		

Control ID	**AC-4(12)**	Control Name	**DATA TYPE IDENTIFIERS**
Definition	When transferring information between different security or privacy domains, use [Assignment: organization-defined data type identifiers] to validate data essential for information flow decisions.		
IHGIN Response	IHGIN disallows specific file types from being used and transferred between systems and privacy domains. Controls for file type identifiers exist within multiple systems to ensure compliance.		

Control ID	**AC-4(13)**	Control Name	**DECOMPOSITION INTO POLICY-RELEVANT SUBCOMPONENTS**
Definition	When transferring information between different security or privacy domains, decompose information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.		
IHGIN Response	Data is analyzed based upon different subcomponents including source, destination, file-type, user roles, and other differentiators to ensure data governance complies with privacy regulations.		

Control ID	**AC-4(14)**	Control Name	**SECURITY OR PRIVACY POLICY FILTER CONSTRAINTS**
Definition	When transferring information between different security or privacy domains, implement [Assignment: organization-defined security or privacy policy filters] requiring fully enumerated formats that restrict data structure and content.		
IHGIN Response	IHGIN has security filter constraints on incoming files and data to ensure that data inputs meet systems requirements. Character sets are restricted and data fields are set to only accept valid strings of data.		

Control ID	**AC-4(15)**	Control Name	**DETECTION OF UNSANCTIONED INFORMATION**
Definition	When transferring information between different security or privacy domains, examine the information for the presence of [Assignment: organization-defined unsanctioned information] and prohibit the transfer of such information in accordance with the [Assignment: organization-defined security or privacy policy].		

IHGIN Response	Data is scanned to determine if data contains sensitive information. Any exfiltration of this data is blocked and flagged for review by IT. Data coming into the organization that contains this information is initially quarantined until released by IT.

Control ID	**AC-4(16)**	Control Name	**INFORMATION TRANSFERS ON INTERCONNECTED SYSTEMS**
Definition	Deprecated (Implemented in AC-4)		
IHGIN Response	See response to section AC-4		

Control ID	**AC-4(17)**	Control Name	**DOMAIN AUTHENTICATION**
Definition	Uniquely identify and authenticate source and destination points by [Selection (one or more): organization, system, application, service, individual] for information transfer.		
IHGIN Response	User are authenticated using a domain and a federated trust. Access to customer information is logged at all times using these accounts and monitored in real-time.		

Control ID	**AC-4(18)**	Control Name	**SECURITY ATTRIBUTE BINDING**
Definition	Deprecated (Incorporated into AC-16)		
IHGIN Response	See response to section AC-16		

Control ID	**AC-4(19)**	Control Name	**VALIDATION OF METADATA**
Definition	When transferring information between different security or privacy domains, implement [Assignment: organization-defined security or privacy policy filters] on metadata.		
IHGIN Response	IHGIN utilizes metadata to tag files and information internally to accurately describe the content types. Currently it is not used to restrict data flow, but this can be implemented if required.		

Control ID	**AC-4(20)**	Control Name	**APPROVED SOLUTIONS**
Definition	Employ [Assignment: organization-defined solutions in approved configurations] to control the flow of [Assignment: organization-defined information] across security or privacy domains		
IHGIN Response	IHGIN scans and logs all cross-domain traffic for virus activity and advanced threats. IHGIN does not house classified information so we do not utilize an approved solution for handling of top-secret information by the NSA National Cross Domain Strategy Office. We can implement such a solution if required.		

Control ID	**AC-4(21)**	Control Name	**PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS**
Definition	Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].		

IHGIN Response	IHGIN utilizes separate networks, subnets, and manages connections between them utilizing access control lists and logs all access to a SIEM solution for reporting. Any out of norm activity is flagged and reviewed by IT staff.

Control ID	**AC-4(22)**	Control Name	**ACCESS ONLY**
Definition	Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing any information flow between the different security domains.		
IHGIN Response	Access between different security domains is controlled using role based and user-based access controls. This includes read-only access for specific data types.		

Control ID	**AC-4(23)**	Control Name	**MODIFY NON-RELEASABLE INFORMATION**
Definition	When transferring information between different security domains, modify non-releasable information by implementing [Assignment: organization-defined modification action].		
IHGIN Response	Any modification of data or data types is logged based upon the user and analyzed using our SIEM solution. Any modification of data and transmittal can be flagged for review by IT if deemed necessary.		

Control ID	**AC-4(24)**	Control Name	**INTERNAL NORMALIZED FORMAT**
Definition	When transferring information between different security domains, parse incoming data into an internal normalized format and regenerate the data to be consistent with its intended specification.		
IHGIN Response	Data stored within IHGIN databases is normalized. Incoming data is normalized and follows a specific data format based upon customer and business need.		

Control ID	**AC-4(25)**	Control Name	**DATA SANITIZATION**
Definition	When transferring information between different security domains, sanitize data to minimize [Selection (one or more: delivery of malicious content, command and control of malicious code, malicious code augmentation, and steganography encoded data; spillage of sensitive information] in accordance with [Assignment: organization-defined policy]].		
IHGIN Response	All data storage devices when reaching end of life are sanitized and then destroyed in-line with the IT security policy. All storage devices containing sensitive information are encrypted.		

Control ID	**AC-4(26)**	Control Name	**AUDIT FILTERING ACTIONS**
Definition	When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered.		
IHGIN Response	All access between security domains is audited with our SIEM solution and reviewed on a regular basis to ensure that operational integrity remains in-tact. Incoming and outgoing data transmissions are filtered to ensure that specified data types and content is not leaving the organization, or that malware or malformed data is not being brought into contact with IHGIN systems.		

Control ID	**AC-4(27)**	Control Name	**REDUNDANT/INDEPENDENT FILTERING MECHANISMS**
Definition	When transferring information between different security or privacy domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type		
IHGIN Response	Data types are specified by the customer and incoming transmissions are scanned to ensure that the incoming data meets the established baseline. Anything outside of the baseline is flagged for review by IT staff.		

Control ID	**AC-4(28)**	Control Name	**LINEAR FILTER PIPELINES**
Definition	When transferring information between different security or privacy domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.		
IHGIN Response	IHGIN utilizes access control lists and advanced threat detection to ensure that data transferred between security domains is restricted to only those that require access. Content is scanned to ensure that it does not violate the IT acceptable usage policy and to ensure that no malformed or malicious data is transmitted between security domains.		

Control ID	**AC-4(29)**	Control Name	**FILTER ORCHESTRATION ENGINES**
Definition	When transferring information between different security or privacy domains, employ content filter orchestration engines to ensure that: a) Content filtering mechanisms successfully complete execution without errors; and b) Content filtering actions occur in the correct order and comply with [Assignment: organization-defined policy].		
IHGIN Response	IHGIN ingests all access between security domains into our SIEM solution. The content filter has an established baseline and will automatically block access or alert IT to attempts to conduct data transactions that are outside of the baseline or business norms. The rules for this are specified by IT staff and actions utilize an orchestration engine to take appropriate action depending upon the time of day.		

Control ID	**AC-4(30)**	Control Name	**FILTER MECHANISMS USING MULTIPLE PROCESSES**
Definition	When transferring information between different security or privacy domains, implement content filtering mechanisms using multiple processes		
IHGIN Response	The advanced security appliance, intrusion detection system, cloud based monitoring, and internal SIEM solution all monitor content to ensure that compliance to the IHGIN security policy is adhered to.		

Control ID	**AC-4(31)**	Control Name	**FAILED CONTENT TRANSFER PREVENTION**
Definition	When transferring information between different security or privacy domains, prevent the transfer of failed content to the receiving domain.		
IHGIN Response	Content transfer if determined to be malicious is blocked by the advanced security appliance. If outside of the baseline of established data it is flagged for review by IT.		

Control ID	**AC-4(32)**	Control Name	**PROCESS REQUIREMENTS FOR INFORMATION TRANSFER**

Definition	When transferring information between different security or privacy domains, the process that transfers information between filter pipelines: a) Does not filter message content; b) Validates filtering metadata; c) Ensures the content associated with the filtering metadata has successfully completed filtering; and d) Transfers the content to the destination filter pipeline
IHGIN Response	The data when transferred is not manipulated in any way. The data transfer between security domains is analyzed in real time to ensure that it meets the specified criteria for transmission. The integrity of the data is maintained through the process.

Control ID	**AC-5**	Control Name	**SEPARATION OF DUTIES**
Definition	a) Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and b) Define system access authorizations to support separation of duties		
IHGIN Response	IHGIN has a clear separation of duties between business roles. This ensures that access is maintained to only those that can show a business need for access to a system or data.		

Control ID	**AC-6**	Control Name	**LEAST PRIVILEGE**
Definition	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.		
IHGIN Response	The principle of least privilege is established in the IHGIN Security Policy and it is strictly adhered to and reviewed on a regular basis.		

Control ID	**AC-6(1)**	Control Name	**AUTHORIZE ACCESS TO SECURITY FUNCTIONS**
Definition	Explicitly authorize access for [Assignment: organization-defined individuals or roles] to: a) [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; and b) [Assignment: organization-defined security-relevant information].		
IHGIN Response	IHGIN strictly adheres to the principle of least privilege and ensures that the IHGIN Security Policy is followed along with internal procedures to ensure that access to security functions is prohibited to only those that need access to a specified resource.		

Control ID	**AC-6(2)**	Control Name	**NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS**
Definition	Require that users of system accounts (or roles) with access to [Assignment: organization defined security functions or security-relevant information], use non-privileged accounts or roles, when accessing nonsecurity functions.		
IHGIN Response	The use of administrative and privileged accounts is restricted to IT staff and these accounts are not to be used for day to day operations of systems. All systems access by privileged accounts is audited and reported on by our SIEM solution.		

Control ID	**AC-6(3)**	Control Name	**NETWORK ACCESS TO PRIVILEGED COMMANDS**
Definition	Authorize network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system.		
IHGIN Response	Network access is restricted based upon IP address and the user account accessing the system.		

Control ID	**AC-6(4)**	Control Name	**SEPARATE PROCESSING DOMAINS**
Definition	Provide separate processing domains to enable finer-grained allocation of user privileges.		
IHGIN Response	IHGIN utilizes virtualization and hyperconverged infrastructure to separate user privileges from the hardware and hypervisor and software layers of systems.		

Control ID	**AC-6(5)**	Control Name	**PRIVILEGED ACCOUNTS**
Definition	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].		
IHGIN Response	Privileged accounts are restricted from being used as day-to-day accounts for access to systems and are restricted to IT staff only. These accounts are monitored and the usage of these accounts is restricted to conducting administrative functions only.		

Control ID	**AC-6(6)**	Control Name	**PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS**
Definition	Prohibit privileged access to the system by non-organizational users.		
IHGIN Response	Privileged access is controlled to organizational IT staff only. In the case where an outside contractor or support personnel will require administrative access to conduct a function, IT staff are to conduct that function for them and monitor the user during their access to any systems. All access is logged and monitored by our SIEM solution.		

Control ID	**AC-6(7)**	Control Name	**REVIEW OF USER PRIVILEGES**
Definition	a) Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and b) Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.		
IHGIN Response	The IHGIN Security Policy explicitly outlines the review period required for user access to systems. User access is removed as necessary to reflect any organizational changes.		

Control ID	**AC-6(8)**	Control Name	**PRIVILEGE LEVELS FOR CODE EXECUTION**
Definition	Prevent the following software from executing at higher privilege levels than users executing the software: [Assignment: organization-defined software].		
IHGIN Response	Software is restricted to being run at a user level. If administrative permissions are required by software for code execution the software is configured with the principle of least privilege in-line with the vendor's specifications. Any access or usage of that account is monitored by our SIEM solution to ensure it adheres to an established baseline of usage.		

Control ID	**AC-6(9)**	Control Name	**LOG USE OF PRIVILEGED FUNCTIONS**
Definition	Audit the execution of privileged functions.		
IHGIN Response	All privileged account functions are audited and logged.		

Control ID	**AC-6(10)**	Control Name	**PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS**
Definition	Prevent non-privileged users from executing privileged functions.		
IHGIN Response	Privileged functions are account locked and the execution of privileged functions requires access to a privileged account. All access is logged and report on.		

Control ID	**AC-7**	Control Name	**UNSUCCESSFUL LOGON ATTEMPTS**
Definition	a) Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time-period]; and b) Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time-period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.		
IHGIN Response	Unsuccessful user logons are logged and monitored by our SIEM solution. Additionally, an account-lockout policy is specified within our IHGIN security policy. Consecutive account lockouts are flagged by IT for review.		

Control ID	**AC-7(1)**	Control Name	**AUTOMATIC ACCOUNT LOCK**
Definition	Deprecated (Implemented in AC-7)		
IHGIN Response	See response to section AC-7		

Control ID	**AC-7(2)**	Control Name	**PURGE OR WIPE MOBILE DEVICE**
Definition	Purge or wipe information from [Assignment: organization-defined mobile devices] based on [Assignment: organization-defined purging or wiping requirements and techniques] after [Assignment: organization-defined number] consecutive, unsuccessful device logon attempts.		

IHGIN Response	Mobile devices are locked after several consecutive unsuccessful logon attempts and must be unlocked by IT staff remotely. IT staff have the option of conducting a remote wipe if they believe the user's device is compromised or being used by an unauthorized user.

Control ID	**AC-7(3)**	Control Name	**BIOMETRIC ATTEMPT LIMITING**
Definition	Limit the number of unsuccessful biometric logon attempts to [Assignment: organization defined number].		
IHGIN Response	As with passwords, any 2 factor authentication will lock the device if the threshold for unsuccessful logon attempts is reached in accordance with the IHGIN Security Policy.		

Control ID	**AC-7(4)**	Control Name	**USE OF ALTERNATE FACTOR**
Definition	a) Allow the use of [Assignment: organization-defined authentication factors] that are different from the primary authentication factors after the number of defined consecutive invalid logon attempts have been exceeded; and b) Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts through use of the alternative factors by a user during a [Assignment: organization-defined time-period].		
IHGIN Response	Certain systems require the use of two-factor authentication to access in accordance with the IHGIN Security Policy.		

Control ID	**AC-8**	Control Name	**System Use Notification**
Definition	a) Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that: 1. Users are accessing a U.S. Government system; 2. System usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and 4. Use of the system indicates consent to monitoring and recording; b) Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and c) For publicly accessible systems: 1. Display system use information [Assignment: organization-defined conditions], before granting further access to the publicly accessible system; 2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Include a description of the authorized uses of the system		
IHGIN Response	Internal IHGIN systems contain banner messages that inform users that access is logged and restricted to IHGIN staff or IT staff as required. External systems are logged, but a banner message is not displayed at this time. This can be implemented as required.		

Control ID	**AC-9**	Control Name	**Previous Logon Notification**
Definition	Notify the user, upon successful logon to the system, of the date and time of the last logon.		
IHGIN Response	Some IHGIN systems will notify the user of the previous logon to their account. These systems are configured to do so if they allow for this functionality. If required this can be rolled out to all systems.		

Control ID	**AC-9(1)**	Control Name	**UNSUCCESSFUL LOGONS**
Definition	Notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon		
IHGIN Response	Unsuccessful logon attempts are monitored by IT staff and the SIEM solution. Users are not notified of unsuccessful logon attempts at this time. This can be configured if required.		

Control ID	**AC-9(2)**	Control Name	**SUCCESSFUL AND UNSUCCESSFUL LOGONS**
Definition	Notify the user, upon successful logon, of the number of [Selection: successful logons; unsuccessful logon attempts; both] during [Assignment: organization-defined time-period].		
IHGIN Response	Unsuccessful and successful logon attempts are monitored by IT staff and the SIEM solution. Users are not notified of unsuccessful logon attempts at this time. This can be configured if required.		

Control ID	**AC-9(3)**	Control Name	**NOTIFICATION OF ACCOUNT CHANGES**
Definition	Notify the user, upon successful logon, of changes to [Assignment: organization-defined security-related characteristics or parameters of the user's account] during [Assignment: organization-defined time-period].		
IHGIN Response	Account changes and administrative functions are logged to the internal SIEM solution. Users are not made aware of account changes by IT staff and any changes to account access not conducted by IT staff is strictly prohibited and reported upon.		

Control ID	**AC-9(4)**	Control Name	**ADDITIONAL LOGON INFORMATION**
Definition	Notify the user, upon successful logon, of the following additional information: [Assignment: organization-defined additional information].		
IHGIN Response	Unsuccessful and successful logon attempts are monitored by IT staff and the SIEM solution. Users are not notified of successful logon attempts at this time. Therefore, additional information is not provided. This can be configured if required.		

Control ID	**AC-10**	Control Name	**Concurrent Session Control**
Definition	Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].		

IHGIN Response	Concurrent sessions are limited based upon the account type and required access to systems.

Control ID	**AC-11**	Control Name	**Device Lock**
Definition	a) Prevent further access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time-period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]; and b) Retain the device lock until the user reestablishes access using established identification and authentication procedures.		
IHGIN Response	Systems are automatically locked for a duration of time outlined in the IHGIN Security Policy. The device lock is maintained until the user re-authenticates to the domain.		

Control ID	**AC-11(1)**	Control Name	**PATTERN-HIDING DISPLAYS**
Definition	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.		
IHGIN Response	Upon locking the device, the screen goes blank or displays a friendly image and not the users desktop or device information.		

Control ID	**AC-12**	Control Name	**SESSION TERMINATION**
Definition	Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].		
IHGIN Response	User sessions are terminated on certain systems after a period of inactivity outlined in the IHGIN Security Policy.		

Control ID	**AC-12(1)**	Control Name	**USER-INITIATED LOGOUTS**
Definition	Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources].		
IHGIN Response	Users have the capability to login and logout of systems where authentication is utilized.		

Control ID	**AC-12(2)**	Control Name	**TERMINATION MESSAGE**
Definition	Display an explicit logout message to users indicating the termination of authenticated communications sessions.		
IHGIN Response	The user will be displayed a message that they are being logged out of the system followed by a successful message.		

Control ID	**AC-12(3)**	Control Name	**TIMEOUT WARNING MESSAGE**
Definition	Display an explicit message to users indicating that the session will end in [Assignment: organization-defined time until end of session]		
IHGIN Response	For online/web-based systems, users will receive a message that their session is about to expire. For other systems, no warning is given. A warning can be configured across all systems if required.		

Control ID	**AC-13**	Control Name	**Supervision and Review-Access Control**
Definition	Deprecated (Incorporated into AC-2 & AU-6)		
IHGIN Response	See response to AC-2 & AU-6		

Control ID	**AC-14**	Control Name	**Permitted Actions without Identification or Authentication**
Definition	a) Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational missions and business functions; and b) Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication		
IHGIN Response	User actions on systems require authentication when done at the software level. Any hardware based changes are logged by IT staff and are restricted to IT staff only.		

Control ID	**AC-14(1)**	Control Name	**NECESSARY USES**
Definition	Deprecated (incorporated into AC-14)		
IHGIN Response	See response to AC-14		

Control ID	**AC-15**	Control Name	**Automated Marking**
Definition	Deprecated (incorporated into MP-3)		
IHGIN Response	See response to MP-3		

Control ID	**AC-16**	Control Name	**Security and Privacy Attributes**
Definition	a) Provide the means to associate [Assignment: organization-defined types of security and privacy attributes] having [Assignment: organization-defined security and privacy attribute values] with information in storage, in process, and/or in transmission; b) Ensure that the attribute associations are made and retained with the information; c) Establish the permitted [Assignment: organization-defined security and privacy attributes] for [Assignment: organization-defined systems]; d) Determine the permitted [Assignment: organization-defined values or ranges] for each of the established attributes; e) Audit changes to attributes; and f) Review [Assignment: organization-defined security and privacy attributes] for applicability [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN specifies security and privacy attributes on user and operator accounts and uses these attributes to assign and audit permissions to assets based upon the organizational security policy.		

Control ID	**AC-16(1)**	Control Name	**DYNAMIC ATTRIBUTE ASSOCIATION**
Definition	Dynamically associate security and privacy attributes with [Assignment: organization defined subjects and objects] in accordance with the following security and privacy policies as information is created and combined: [Assignment: organization-defined security and privacy policies].		
IHGIN Response	Some user account attributes are inherited, and they dynamically change based upon group membership in accordance with the IHGIN Security Policy.		

Control ID	**AC-16(2)**	Control Name	**ATTRIBUTE VALUE CHANGES BY AUTHORIZED INDIVIDUALS**
Definition	Provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security and privacy attributes		
IHGIN Response	IT administrators are the only individuals with access to make these changes. These changes are approved by a manager prior to implementation and all account changes are audited.		

Control ID	**AC-16(3)**	Control Name	**MAINTENANCE OF ATTRIBUTE ASSOCIATIONS BY SYSTEM**
Definition	Maintain the association and integrity of [Assignment: organization-defined security and privacy attributes] to [Assignment: organization-defined subjects and objects].		
IHGIN Response	The SIEM solution audits the user attributed to ensure that they are not outside of the baseline established. When changes, the SIEM solution will flag the change in permissions for review automatically until a new baseline is established for that user.		

Control ID	**AC-16(4)**	Control Name	**ASSOCIATION OF ATTRIBUTES BY AUTHORIZED INDIVIDUALS**
Definition	Provide the capability to associate [Assignment: organization-defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] by authorized individuals (or processes acting on behalf of individuals).		
IHGIN Response	Only privileged IT accounts can make changes to user attributes within our system. IT administrative accounts can make changes to user attributes as needed.		

Control ID	**AC-16(5)**	Control Name	**ATTRIBUTE DISPLAYS FOR OUTPUT DEVICES**
Definition	Display security and privacy attributes in human-readable form on each object that the system transmits to output devices to identify [Assignment: organization-defined special dissemination, handling, or distribution instructions] using [Assignment: organization defined human-readable, standard naming conventions].		
IHGIN Response	No personal information is displayed on screens in a public area. If there is a need for this, controls can be put in place to ensure compliance.		

Control ID	**AC-16(6)**	Control Name	**MAINTENANCE OF ATTRIBUTE ASSOCIATION BY ORGANIZATION**
Definition	Require personnel to associate and maintain the association of [Assignment: organization defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security and privacy policies].		
IHGIN Response	IT staff are responsible for the maintenance of user attributes.		

Control ID	**AC-16(7)**	Control Name	**CONSISTENT ATTRIBUTE INTERPRETATION**
Definition	Provide a consistent interpretation of security and privacy attributes transmitted between distributed system components		
IHGIN Response	Active directory is used to control access based upon user attributes.		

Control ID	**AC-16(8)**	Control Name	**ASSOCIATION TECHNIQUES AND TECHNOLOGIES**
Definition	Implement [Assignment: organization-defined techniques and technologies] with [Assignment: organization-defined level of assurance] in associating security and privacy attributes to information.		
IHGIN Response	Attributes are used within Active Directory, we currently do not use cryptographic technology to accomplish this control. It can be implemented if necessary.		

Control ID	**AC-16(9)**	Control Name	**ATTRIBUTE REASSIGNMENT – REGRADING MECHANISMS**
Definition	Change security and privacy attributes associated with information only via regrading mechanisms validated using [Assignment: organization-defined techniques or procedures].		
IHGIN Response	We currently do not utilize this control as we have no business need to do so. If required it can be implemented.		

Control ID	**AC-16(10)**	Control Name	**ATTRIBUTE CONFIGURATION BY AUTHORIZED INDIVIDUALS**
Definition	Provide authorized individuals the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects.		
IHGIN Response	IT administrative staff have the capability to make changes to user attributes. These changes are logged and monitored using our SIEM solution.		

Control ID	**AC-17**	Control Name	**REMOTE ACCESS**
Definition	a) Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b) Authorize each type of remote access to the system prior to allowing such connections		
IHGIN Response	Remote access to systems and the requirements for encryption are laid out in the IHGIN Security Policy.		

Control ID	**AC-17(1)**	Control Name	**MONITORING AND CONTROL**
Definition	Employ automated mechanisms to monitor and control remote access methods		
IHGIN Response	Remote access is audited and monitored using our SIEM solution. Any access outside of the baseline is flagged for review or immediately terminated based upon the time of day.		

Control ID	**AC-17(2)**	Control Name	**PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION**

Definition	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
IHGIN Response	Cryptographic requirements are laid out specifically in the IHGIN Security Policy. All data is encrypted in transit and at rest.

Control ID	**AC-17(3)**	Control Name	**MANAGED ACCESS CONTROL POINTS**
Definition	Route remote accesses through authorized and managed network access control points.		
IHGIN Response	All remote access is authorized and managed through our firewalls and monitored.		

Control ID	**AC-17(4)**	Control Name	**PRIVILEGED COMMANDS AND ACCESS**
Definition	a) Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs]; and b) Document the rationale for remote access in the security plan for the system		
IHGIN Response	Remote access requires two-factor authentication. IT Administrator access is restricted by ip address into our network and monitors for any changes that are made while connected.		

Control ID	**AC-17(5)**	Control Name	**MONITORING FOR UNAUTHORIZED CONNECTIONS**
Definition	Deprecated (Implemented into SI-4)		
IHGIN Response	See response to SI-4		

Control ID	**AC-17(6)**	Control Name	**PROTECTION OF MECHANISM INFORMATION**
Definition	Protect information about remote access mechanisms from unauthorized use and disclosure.		
IHGIN Response	If access by a third party is required remotely to IHGIN resources, an agreement on the technical requirements and acceptable usage is defined prior to access.		

Control ID	**AC-17(7)**	Control Name	**ADDITIONAL PROTECTION FOR SECURITY FUNCTION ACCESS**
Definition	Deprecated (Implemented into AC-3(10))		
IHGIN Response	See response to AC-3(10)		

Control ID	**AC-17(8)**	Control Name	**DISABLE NONSECURE NETWORK PROTOCOLS**
Definition	Deprecated (Implemented into CM-7)		
IHGIN Response	See response to CM-7		

Control ID	**AC-17(9)**	Control Name	**DISCONNECT OR DISABLE ACCESS**

Definition	Provide the capability to disconnect or disable remote access to the system within [Assignment: organization-defined time-period].
IHGIN Response	IGHIN IT can disable access or disconnect users at any time for any reason without warning.

Control ID	**AC-17(10)**	Control Name	**AUTHENTICATE REMOTE COMMANDS**
Definition	Implement [Assignment: organization-defined controls] to authenticate [Assignment: organization-defined remote commands].		
IHGIN Response	Cryptographic controls are implemented as outlined in the IHGIN Security Policy to ensure that all remote access and commands are authenticated and encrypted.		

Control ID	**AC-18**	Control Name	**Wireless Access**
Definition	a) Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and b) Authorize each type of wireless access to the system prior to allowing such connections.		
IHGIN Response	Wireless access controls and user requirements are specified in the IHGIN Security Policy. The wireless network is air-gapped from the corporate network and any users on the wireless network must use a secure vpn tunnel to gain access to company resources.		

Control ID	**AC-18(1)**	Control Name	**AUTHENTICATION AND ENCRYPTION**
Definition	Protect wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.		
IHGIN Response	Wireless access is encrypted and users have to authenticate with a password. The wireless network only provides an internet connection and no access to corporate resources.		

Control ID	**AC-18(2)**	Control Name	**MONITORING UNAUTHORIZED CONNECTIONS**
Definition	Deprecated (Implemented into SI-4)		
IHGIN Response	See response to SI-4		

Control ID	**AC-18(3)**	Control Name	**DISABLE WIRELESS NETWORKING**
Definition	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.		
IHGIN Response	Any computer not using a wireless connection has the wireless card disabled on the device. Administrative privileges reserved for IT staff is required to enable the wireless connection.		

Control ID	**AC-18(4)**	Control Name	**RESTRICT CONFIGURATIONS BY USERS**
Definition	Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.		

IHGIN Response	Only IT administrators can configure wireless access for users.

Control ID	**AC-18(5)**	Control Name	**ANTENNAS AND TRANSMISSION POWER LEVELS**
Definition	Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.		
IHGIN Response	Radio antenna power is adjusted to ensure that wireless access is not accessible off-property. The wireless network is monitored for new users and any new users are flagged for approval by IT prior to being given access.		

Control ID	**AC-19**	Control Name	**Access Control for Mobile Devices**
Definition	a) Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and b) Authorize the connection of mobile devices to organizational systems		
IHGIN Response	IHGIN uses a mobile device management solution that enforces configuration and connection requirements in-line with the IHGIN Security Policy on corporate owned mobile devices.		

Control ID	**AC-19(1,2,3)**	Control Name	**Storage devices**
Definition	Deprecated (Implemented in MP-7)		
IHGIN Response	Please see response to MP-7		

Control ID	**AC-19(4)**	Control Name	**RESTRICTIONS FOR CLASSIFIED INFORMATION**
Definition	a) Prohibit the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and b) Enforce the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information: 1. Connection of unclassified mobile devices to classified systems is prohibited; 2. Connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official; 3. Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and 4. Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed. c) Restrict the connection of classified mobile devices to classified systems in accordance with [Assignment: organization-defined security policies].		

IHGIN Response	IHGIN does not work with classified information, this control is not implemented at tis time. This can be implemented if required.

Control ID	**AC-19(5)**	Control Name	**FULL DEVICE AND CONTAINER-BASED ENCRYPTION**
Definition	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].		
IHGIN Response	Mobile devices are encrypted to protect the integrity of the information stored on the devices. This is enforced through our mobile device management solution.		

Control ID	**AC-20**	Control Name	**Use of External Systems**
Definition	Establish [Selection (one or more): [Assignment: organization-defined terms and conditions]; [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to: a. Access the system from external systems; and b. Process, store, or transmit organization-controlled information using external systems		
IHGIN Response	Prior to allowing external systems to be utilized within the environment they must first be vetted by IT staff to ensure they meet our compliance requirements. These systems are then allowed and monitored to ensure that traffic does not go outside of an established baseline. Customer information is only transferred to external systems as dictated by the customer and never shared with a third party without explicit instruction to do so.		

Control ID	**AC-20(1)**	Control Name	**LIMITS ON AUTHORIZED USE**
Definition	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after: a) Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or b) Retention of approved system connection or processing agreements with the organizational entity hosting the external system.		
IHGIN Response	Externally systems that require usage are asked to provide a verifiable list of controls that are in place as it pertains to the data being transferred between the systems. Typically, a copy of the information security policy along with any recent audits is requested to fulfill this need. Additionally, the connection is actively monitored against an established baseline to ensure that traffic and data does not go outside of the scope of what is to be transferred.		

Control ID	**AC-20(2)**	Control Name	**PORTABLE STORAGE DEVICES — RESTRICTED USE**
Definition	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions].		

IHGIN Response	The use of portable storage devices is limited under the IHGIN Security Policy. Users are not allowed to use portable storage devices on systems containing sensitive information. In the case that a client requires this to be used to transmit data, the movement of files to the device is conducted by IT staff and a chain of custody is maintained.

Control ID	**AC-20(3)**	Control Name	**NON-ORGANIZATIONALLY OWNED SYSTEMS — RESTRICTED USE**
Definition	Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using [Assignment: organization-defined restrictions].		
IHGIN Response	The storage of information on non-organizationally owned systems is prohibited.		

Control ID	**AC-20(4)**	Control Name	**NETWORK ACCESSIBLE STORAGE DEVICES**
Definition	Prohibit the use of [Assignment: organization-defined network accessible storage devices] in external systems.		
IHGIN Response	Externally owned systems are segmented to their own broadcast domain and any traffic from these systems to internal systems is routed through the security appliance and audited.		

Control ID	**AC-20(5)**	Control Name	**PORTABLE STORAGE DEVICES — PROHIBITED USE**
Definition	Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems		
IHGIN Response	Portable storage devices are disabled by default on all machines in the IHGIN environment. The use of these devices is controlled by IT staff when a business need to do so arises. Any portable storage device that has touched an external device will not be used.		

Control ID	**AC-20(6)**	Control Name	**NON-ORGANIZATIONALLY OWNED SYSTEMS — PROHIBITED USE**
Definition	Prohibit the use of non-organizationally owned systems or system components to process, store, or transmit organizational information.		
IHGIN Response	Non-organizationally owned systems are vetted prior to being utilized within the IHGIN environment. These systems are segregated to their own broadcast domains and access is controlled through the firewall. Any system being implemented is vetted by IT staff and a risk assessment done to ensure that organizational data is protected. Any non-IT approved third party systems are prohibited from use on the IHGIN network.		

Control ID	**AC-21**	Control Name	**Information Sharing**
Definition	a) Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization defined information sharing circumstances where user discretion is required]; and		

	b) Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions
IHGIN Response	Internal customer data is prohibited from being shared externally without prior approval from the customer. Users can share internal corporate documents and information with other staff members through Sharepoint, but all access is logged and audited to ensure that integrity and confidentiality of the documents remain in-tact. Any shared document within Sharepoint automatically expires after a period of time outlined in the IHGIN Security Policy.

Control ID	**AC-21(1)**	Control Name	**AUTOMATED DECISION SUPPORT**
Definition	Employ [Assignment: organization-defined automated mechanisms] to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared		
IHGIN Response	Sharing externally is disabled in Sharepoint and will generate an alert if attempted by a user. Automation is setup to disable shared links after a period of time outlined in the IHGIN Security Policy.		

Control ID	**AC-21(2)**	Control Name	**INFORMATION SEARCH AND RETRIEVAL**
Definition	Implement information search and retrieval services that enforce [Assignment: organization-defined information sharing restrictions].		
IHGIN Response	Internal search capabilities are limited only to files a user has access to.		

Control ID	**AC-22**	Control Name	**Publicly Accessible Content**
Definition	a) Designate individuals authorized to make information publicly accessible; b) Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; c) Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and d) Review the content on the publicly accessible system for nonpublic information [Assignment: organization-defined frequency] and remove such information, if discovered		
IHGIN Response	Prior to information being made public, the data is reviewed by management to ensure that the information contained does not expose the organization or customers to any risk. The data is then scrubbed of metadata to ensure that metadata leakage does not happen to external facing documents. The amount of information made public is extremely limited.		

Control ID	**AC-23**	Control Name	**Data Mining Protection**
Definition	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.		

IHGIN Response	IHGIN uses access control lists to customer facing sites and content to ensure that only the customer can access those sites. They are monitored using our SIEM solution to ensure that traffic adheres to the normal user traffic. Our public facing website has limited information posted to ensure that organizational data remains private. The robots.txt file is used to limit access to unpublished sections of the website and the website is monitored to ensure that any abnormal use of the website is reviewed.

Control ID	**AC-24**	Control Name	**Access Control Decisions**
Definition	[Selection: Establish procedures; Implement mechanisms] to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.		
IHGIN Response	Access control to customer facing systems is determined by the contracted needs of the customer and access controls such as access control lists and accounts are configured by IT staff to enforce the principle of least access.		

Control ID	**AC-24(1)**	Control Name	**TRANSMIT ACCESS AUTHORIZATION INFORMATION**
Definition	Transmit [Assignment: organization-defined access authorization information] using [Assignment: organization-defined controls] to [Assignment: organization-defined systems] that enforce access control decisions		
IHGIN Response	Passwords are given to customers over the phone only, and their username is sent to them electronically.		

Control ID	**AC-24(2)**	Control Name	**NO USER OR PROCESS IDENTITY**
Definition	Enforce access control decisions based on [Assignment: organization-defined security or privacy attributes] that do not include the identity of the user or process acting on behalf of the user.		
IHGIN Response	Users are required to verify their identity with customer service prior to having a password change conducted. Any access control change has to be processed by IT, and additional information may be required from the customer to ensure that their privacy is protected and their identity verified.		

Control ID	**AC-25**	Control Name	**Reference Monitor**
Definition	Implement a reference monitor for [Assignment: organization-defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured		
IHGIN Response	IHGIN utilizes a baseline reference monitor for every user and system internally that is specified to that system. AI is then used to determine if actions are conducted outside of that baselined data and flagged as such for review or access is automatically limited.		

Awareness and Training

Control ID	**AT-1**	Control Name	**POLICY AND PROCEDURES**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:		

	1. [Selection (one or more): organization-level; mission/business process-level; system level] awareness and training policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and c) Review and update the current awareness and training: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	IHGIN conducts regular cyber security awareness training in-line with the requirements outlined in the IHGIN Security Policy. All staff must accept the IHGIN Acceptable Usage Policy prior to gaining network access. Upon receipt of training staff sign off showing that they understand the training they had received. Staff are tested randomly throughout the year to ensure they remain compliant and take proper care to protect customer information. If a staff member fails the random test they are required to review the IHGIN Security Policy and are flagged to receive cyber security training at the next available date.

Control ID	**AT-2**	Control Name	**Awareness Training**
Definition	a) Provide security and privacy awareness training to system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and 2. When required by system changes; and b) Update awareness training [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN requires all staff to take part in cyber security awareness training on a regular basis as outlined in the IHGIN Security Policy.		

Control ID	**AT-2(1)**	Control Name	**PRACTICAL EXERCISES**
Definition	Provide practical exercises in awareness training that simulate events and incidents		
IHGIN Response	IHGIN IT staff will randomly test staff through the year without notice with simulated events and incidents to ensure compliance with the IHGIN Security Policy. Training uses exercises and videos to showcase how easy it is to fall victim to a cyber event.		

Control ID	**AT-2(2)**	Control Name	**INSIDER THREAT**
Definition	Provide awareness training on recognizing and reporting potential indicators of insider threat.		

IHGIN Response	Staff are reminded during training that if they suspect anyone of doing something wrong with the network that they are to contact IT staff immediately. Any information passed to IT staff remains confidential on these items during the investigation.

Control ID	**AT-2(3)**	Control Name	**SOCIAL ENGINEERING AND MINING**
Definition	Provide awareness training on recognizing and reporting potential and actual instances of social engineering and social mining.		
IHGIN Response	Social engineering exercises are a large component of the IHGIN security awareness training.		

Control ID	**AT-2(4)**	Control Name	**SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR**
Definition	Provide awareness training on recognizing suspicious communications and anomalous behavior in organizational systems using [Assignment: organization-defined indicators of malicious code].		
IHGIN Response	IHGIN staff are trained on how to recognize suspicious behavior and anomalous system behavior. They are to contact IT at any time if they have any questions.		

Control ID	**AT-2(5)**	Control Name	**BREACH**
Definition	Provide awareness training on how to identify and respond to a breach, including the organization's process for reporting a breach.		
IHGIN Response	IHGIN has outlined the internal procedures for a response to a breach in the IHGIN disaster recovery plan. Reporting of the breach to the customer is done by the account representative immediately upon discovery and ongoing communications and reporting is done as required.		

Control ID	**AT-2(6)**	Control Name	**ADVANCED PERSISTENT THREAT**
Definition	Provide awareness training on the advanced persistent threat.		
IHGIN Response	IHGIN staff are aware of the concept of the advanced persistent threat and what damage can be done through an APT.		

Control ID	**AT-2(7)**	Control Name	**CYBER THREAT ENVIRONMENT**
Definition	a. Provide awareness training on the cyber threat environment; and b. Reflect current cyber threat information in system operations.		
IHGIN Response	The Cyber Threat Environment is reviewed with staff to ensure they understand the risks associated with internet connected devices. The cyber threat environment is evolving, and this information changes during each training session.		

Control ID	**AT-2(8)**	Control Name	**TRAINING FEEDBACK**
Definition	Provide feedback on organizational training results to the following personnel [Assignment: organization-defined frequency]: [Assignment: organization-defined personnel].		

IHGIN Response	At the end of each training sessions a request for anonymous feedback is given in order to improve upon the content delivered.

Control ID	**AT-3**	Control Name	**Role-Based Training**
Definition	a) Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]: 1. Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and 2. When required by system changes; and b) Update role-based training [Assignment: organization-defined frequency].		
IHGIN Response	Specific security training on systems is given to users with access to customer facing systems.		

Control ID	**AT-3(1)**	Control Name	**ENVIRONMENTAL CONTROLS**
Definition	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of environmental controls.		
IHGIN Response	Training on environmental controls is required by all staff to fully understand plant safety requirements and any fire suppression or environment systems that are in place for employee safety. This safety training is a requirement of all staff prior to beginning work.		

Control ID	**AT-3(2)**	Control Name	**PHYSICAL SECURITY CONTROLS**
Definition	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.		
IHGIN Response	Training on the importance and safe usage of physical security controls is part of the employee onboarding program. Training on the use of physical security controls and the importance of maintaining them is given prior to staff beginning work.		

Control ID	**AT-3(3)**	Control Name	**PRACTICAL EXERCISES**
Definition	Provide practical exercises in security and privacy training that reinforce training objectives.		
IHGIN Response	Ongoing random testing of security systems and policies is conducted by IT and facilities staff to ensure staff compliance.		

Control ID	**AT-3(4)**	Control Name	**SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR**
Definition	Deprecated (Implemented in AT-2(4))		
IHGIN Response	See response to AT-2(4)		

Control ID	**AT-3(5)**	Control Name	**ACCESSING PERSONALLY IDENTIFIABLE INFORMATION**
Definition	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training on: a. Organizational authority for collecting personally identifiable information; b. Authorized uses of personally identifiable information; c. Identifying, reporting, and responding to a suspected or confirmed breach; d. Content of system of records notices, computer matching agreements, and privacy impact assessments; e. Authorized sharing of personally identifiable information with external parties; and f. Rules of behavior and the consequences for unauthorized collection, use, or sharing of personally identifiable information		
IHGIN Response	IT staff are trained explicitly on handling data breaches and the disaster recovery process and roles there-in are practices on an annual basis to ensure that staff are aware of their requirement in the case of a breach or inappropriate access of personally identifiable information. Staff that access systems containing PII are trained on their roles to help protect that information.		

Control ID	**AT-4**	Control Name	**Training Records**
Definition	a) Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and b) Retain individual training records for [Assignment: organization-defined time-period].		
IHGIN Response	Training records are maintained for a period of 7 years.		

Control ID	**AT-5**	Control Name	**Contacts with Security Groups and Associations**
Definition	Deprecated (Implemented in PM-15)		
IHGIN Response	See response to PM-15		

Audit and Accountability

Control ID	**AU-1**	Control Name	**POLICY AND PROCEDURES**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] audit and accountability policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and		

	b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and c) Review and update the current audit and accountability 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	Auditing requirements are outlined in the IHGIN Security Policy. All systems access and data manipulation is logged and audited using our SIEM solution. The auditing of systems is setup based upon systems capabilities and updated when the IHGIN Security Policy is updated, or at such a time that new technology is introduced into the network that has advanced auditing capabilities. Internal software is developed with auditing capabilities created in-line with the IHGIN Security Policy.

Control ID	**AU-2**	Control Name	**Event Logging**
Definition	a) Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging]; b) Coordinate the event logging function with other organizational entities requiring audit related information to guide and inform the selection criteria for events to be logged; c) Specify the following event types for logging within the system: [Assignment: organization defined event types (subset of the event types defined in AU-2 a.) along with the frequency of (or situation requiring) logging for each identified event type]; d) Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and e) Review and update the event types selected for logging [Assignment: organization-defined frequency].		
IHGIN Response	Event logging is controlled by group policy objects and the SIEM solution ingests event logs from systems and analyzes them. Advanced event logging is configured to ensure that users access to systems, object access, policy change, or privileged use is logged and analyzed by our SIEM solution		

Control ID	**AU-2(1-4)**	Control Name	**Audit & Records**
Definition	Deprecated (Implemented in AU-12, AU-2, & AC-6(9))		
IHGIN Response	See response to AU-12, AU2, & AC-6(9)		

Control ID	**AU-3**	Control Name	**Content of Audit Records**
Definition	Ensure that audit records contain information that establishes the following: a. What type of event occurred;		

	b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or objects/entities associated with the event
IHGIN Response	The audit records contain this information.

Control ID	**AU-3(1)**	Control Name	**ADDITIONAL AUDIT INFORMATION**
Definition	Generate audit records containing the following additional information: [Assignment: organization-defined additional information].		
IHGIN Response	Additional audit information is configured based upon systems ability and outlined in the IHGIN Security Policy.		

Control ID	**AU-3(2)**	Control Name	**CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT**
Definition	Provide centralized management and configuration of the content to be captured in audit records generated by [Assignment: organization-defined system components].		
IHGIN Response	All audit records and logs are collected by our SIEM solution and analyzed in near real-time to ensure that individuals remain compliant with the IHGIN Security Policy.		

Control ID	**AU-3(3)**	Control Name	**LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS**
Definition	Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements]		
IHGIN Response	No PII is contained in audit records.		

Control ID	**AU-4**	Control Name	**Audit Log Storage Capacity**
Definition	Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].		
IHGIN Response	IHGIN has substantial audit log storage capacity and expands storage as needed.		

Control ID	**AU-4(1)**	Control Name	**TRANSFER TO ALTERNATE STORAGE**
Definition	Transfer audit logs [Assignment: organization-defined frequency] to a different system, system component, or media other than the system or system component conducting the logging.		
IHGIN Response	A collector is used to collect audit logs and information prior to being analyzed by our SIEM solution. This collector is setup in fault tolerant environment to ensure that it remains operational at all times.		

Control ID	**AU-5**	Control Name	**Response to Audit Logging Process Failures**
Definition	a) Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time-period] in the event of an audit logging process failure; and b) Take the following additional actions: [Assignment: organization-defined additional actions].		
IHGIN Response	The SIEM solution alerts IT staff to abnormal user behavior or systems issues and IT staff take action to investigate.		

Control ID	**AU-5(1)**	Control Name	**STORAGE CAPACITY WARNING**
Definition	Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time-period] when allocated audit log storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit log storage capacity.		
IHGIN Response	Systems performance monitoring is done by our SIEM solution and alerts generated for storage capacity issues.		

Control ID	**AU-5(2)**	Control Name	**REAL-TIME ALERTS**
Definition	Provide an alert within [Assignment: organization-defined real-time-period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts].		
IHGIN Response	Alerts are provided in real-time to IT staff.		

Control ID	**AU-5(3)**	Control Name	**CONFIGURABLE TRAFFIC VOLUME THRESHOLDS**
Definition	Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [Selection: reject; delay] network traffic above those thresholds.		
IHGIN Response	Currently there is no limit on network communications traffic as we are not seeing any degradation of performance from log collection. If we reach a point where it is problematic, traffic volume thresholds will be implemented.		

Control ID	**AU-5(4)**	Control Name	**SHUTDOWN ON FAILURE**
Definition	Invoke a [Selection: full system shutdown; partial system shutdown; degraded operational mode with limited mission or business functionality available] in the event of [Assignment: organization-defined audit logging failures], unless an alternate audit logging capability exists.		
IHGIN Response	In the case of systems failure, the audit logging system will shut off and the backup system will act as the primary until resolved. The back-up system will alert for problems on the primary system and vice versa to ensure operational integrity is maintained.		

Control ID	**AU-5(5)**	Control Name	**ALTERNATE AUDIT LOGGING CAPABILITY**
Definition	Provide an alternate audit logging capability in the event of a failure in primary audit logging capability that implements [Assignment: organization-defined alternate audit logging functionality].		
IHGIN Response	The back-up system will alert for problems on the primary system and vice versa to ensure operational integrity is maintained.		

Control ID	**AU-6**	Control Name	**Audit Record Review, Analysis, and Reporting**
Definition	a) Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; b) Report findings to [Assignment: organization-defined personnel or roles]; and c) Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information.		
IHGIN Response	Reports are generated on a weekly basis and reviewed by IT to see if there is anything that the AI did not catch. Additional reports can be generated as operationally needed. The audit logging system is constantly changing to adapt to new risks as outlined by law enforcement of IT security professionals. The audit logging process is reviewed regularly within the IHGIN Security Policy and updated accordingly.		

Control ID	**AU-6(1)**	Control Name	**AUTOMATED PROCESS INTEGRATION**
Definition	Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	Automated record review, analysis, and reporting is built into the SIEM solution.		

Control ID	**AU-6(2)**	Control Name	**AUTOMATED SECURITY ALERTS**
Definition	Deprecated (Implemented into SI-4)		
IHGIN Response	See response to SI-4		

Control ID	**AU-6(3)**	Control Name	**CORRELATE AUDIT RECORD REPOSITORIES**
Definition	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.		
IHGIN Response	All systems capable of auditing are always monitored. This information is correlated using an AI that establishes a baseline both organizationally and individually to each system. Any traffic outside of this baseline is flagged for review by IT staff.		

Control ID	**AU-6(4)**	Control Name	**CENTRAL REVIEW AND ANALYSIS**
Definition	Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.		

IHGIN Response	This is achieved through our SIEM solution.

Control ID	**AU-6(5)**	Control Name	**INTEGRATED ANALYSIS OF AUDIT RECORDS**
Definition	Integrate analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.		
IHGIN Response	This is achieved through our SIEM solution.		

Control ID	**AU-6(6)**	Control Name	**CORRELATION WITH PHYSICAL MONITORING**
Definition	Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.		
IHGIN Response	Physical access logs are maintained on a separate system but utilize a central NTP server to maintain log times. These logs are compared during investigations by IT staff on occasion to ensure that non-repudiation exists within our systems.		

Control ID	**AU-6(7)**	Control Name	**PERMITTED ACTIONS**
Definition	Specify the permitted actions for each [Selection (one or more): system process; role; user] associated with the review, analysis, and reporting of audit record information.		
IHGIN Response	The SIEM solution will analyze to ensure that systems and users do not go outside of their scope. If a system or user is conducting abnormal behavior, IT is notified as such.		

Control ID	**AU-6(8)**	Control Name	**FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS**
Definition	Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.		
IHGIN Response	Full-text analysis is not always available due to encryption. Changes to files and access to the system by privileged users is logged and analyzed in real-time.		

Control ID	**AU-6(9)**	Control Name	**CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES**
Definition	Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.		
IHGIN Response	During investigations non-technical sources and user interviews are used as part of the investigation process.		

Control ID	**AU-6(10)**	Control Name	**AUDIT LEVEL ADJUSTMENT**
Definition	Deprecated (Implemented into AU-6)		
IHGIN Response	See response to AU-6		

Control ID	**AU-7**	Control Name	**Audit Record Reduction and Report Generation**
Definition	Provide and implement an audit record reduction and report generation capability that: a) Supports on-demand audit record review, analysis, and reporting requirements and after the-fact investigations of incidents; and b) Does not alter the original content or time ordering of audit records.		
IHGIN Response	This is achieved through our SIEM solution.		

Control ID	**AU-7(1)**	Control Name	**AUTOMATIC PROCESSING**
Definition	Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records].		
IHGIN Response	Our SIEM solution automatically processes and analyzes all incoming audit records and events for any known threats or abnormal behavior.		

Control ID	**AU-7(2)**	Control Name	**AUTOMATIC SEARCH AND SORT**
Definition	Deprecated (Implemented into AU-7(1))		
IHGIN Response	See response to AU-7(1)		

Control ID	**AU-8**	Control Name	**Time Stamps**
Definition	a) Use internal system clocks to generate time stamps for audit records; and b) Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.		
IHGIN Response	A NTP server is used to synchronize time across all networked devices.		

Control ID	**AU-8(1)**	Control Name	**SYNCHRONIZATION WITH AUTHORITATIVE TIME SOURCE**
Definition	a) Compare the internal system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and b) Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time-period].		
IHGIN Response	Internal systems are monitored for time shift. Network access is rejected if time shift goes 5 minutes outside of the NTP server.		

Control ID	**AU-8(2)**	Control Name	**SECONDARY AUTHORITATIVE TIME SOURCE**
Definition	a) Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source; and		

	b) Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable.
IHGIN Response	There is a backup domain controller that can also act as an NTP server if the main server is down.

Control ID	**AU-9**	Control Name	**Protection of Audit Information**
Definition	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.		
IHGIN Response	Only IT staff have access to the audit log collection and any changes to written audit logs are immediately flagged by the SIEM solution and any accounts or systems associated with the change are blocked from network access until confirmed by IT to be an authorized change. IT does not change audit logs under any circumstance, but some systems may run circular logs that trigger this system and their activity is monitored.		

Control ID	**AU-9(1)**	Control Name	**HARDWARE WRITE-ONCE MEDIA**
Definition	Write audit trails to hardware-enforced, write-once media.		
IHGIN Response	Currently we do not utilize hardware-based WORM storage for long-term storage of logs. We utilize software-based permissions to achieve this control. This can be implemented if required.		

Control ID	**AU-9(2)**	Control Name	**STORE ON SEPARATE PHYSICAL SYSTEMS OR COMPONENTS**
Definition	Store audit records [Assignment: organization-defined frequency] in a repository that is part of a physically different system or system component than the system or component being audited.		
IHGIN Response	Audit logs are stored on a fault tolerant collection system. This system is separate from the physical systems or components generating the logs.		

Control ID	**AU-9(3)**	Control Name	**CRYPTOGRAPHIC PROTECTION**
Definition	Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.		
IHGIN Response	The audit records are encrypted in storage and in passing to the SIEM solution. The collector uses encrypted methods to collect the data where applicable, but not all systems support this functionality.		

Control ID	**AU-9(4)**	Control Name	**ACCESS BY SUBSET OF PRIVILEGED USERS**
Definition	Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].		
IHGIN Response	Only privileged IT staff have access to configure or edit audit logging.		

Control ID	**AU-9(5)**	Control Name	**DUAL AUTHORIZATION**

Definition	Enforce dual authorization for [Selection (one or more): movement; deletion] of [Assignment: organization-defined audit information].
IHGIN Response	Dual authorization is not required at this time for the configuration or change of configuration of audit logging. Any changes are logged and reviewed by a separate IT staff member to ensure that the operational outcome required by the change is achieved. The SIEM solution will automatically flag any auditing changes for review by IT staff.

Control ID	**AU-9(6)**	Control Name	**READ-ONLY ACCESS**
Definition	Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users or roles].		
IHGIN Response	Audit logs are given read-only privileges on the log collection system.		

Control ID	**AU-9(7)**	Control Name	**STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM**
Definition	Store audit information on a component running a different operating system than the system or component being audited.		
IHGIN Response	Audit logs are stored on a fault tolerant collection system. This system is separate from the physical systems or components generating the logs. This system is running on Linux, but it does monitor a small number of Linux based systems as well. A fault-tolerant Windows based log collection system can be configured for these Linux systems if the customer requires that extra level of security.		

Control ID	**AU-10**	Control Name	**Non-repudiation**
Definition	Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non repudiation]		
IHGIN Response	Non-repudiation is achieved through the combination of our physical access logs, camera systems, and audit logs. Investigations utilize chain-of-custody records to ensure that data cannot be put into question during an investigation.		

Control ID	**AU-10(1)**	Control Name	**ASSOCIATION OF IDENTITIES**
Definition	a) Bind the identity of the information producer with the information to [Assignment: organization-defined strength of binding]; and b) Provide the means for authorized individuals to determine the identity of the producer of the information.		
IHGIN Response	This is fully audited across all systems and monitored using our SIEM solution.		

Control ID	**AU-10(2)**	Control Name	**VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY**

Definition	a) Validate the binding of the information producer identity to the information at [Assignment: organization-defined frequency]; and b) Perform [Assignment: organization-defined actions] in the event of a validation error.
IHGIN Response	Checksums and Kreberos tickets are used to achieve this binding.

Control ID	**AU-10(3)**	Control Name	**CHAIN OF CUSTODY**
Definition	Maintain reviewer or releaser identity and credentials within the established chain of custody for information reviewed or released.		
IHGIN Response	During investigations, a chain-of-custody is created to ensure that non-repudiation can be maintained by the organization.		

Control ID	**AU-10(4)**	Control Name	**VALIDATE BINDING OF INFORMATION REVIEWER IDENTITY**
Definition	a) Validate the binding of the information reviewer identity to the information at the transfer or release points prior to release or transfer between [Assignment: organization-defined security domains]; and b) Perform [Assignment: organization-defined actions] in the event of a validation error		
IHGIN Response	Checksums and Kreberos tickets are used to achieve this binding.		

Control ID	**AU-10(5)**	Control Name	**DIGITAL SIGNATURES**
Definition	Deprecated (Implemented in SI-7)		
IHGIN Response	See response to SI-7		

Control ID	**AU-11**	Control Name	**Audit Record Retention**
Definition	Retain audit records for [Assignment: organization-defined time-period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.		
IHGIN Response	Audit records are maintained in-line with regulatory requirements. 7 years of records are maintained in archive. One year is maintained in an active state prior to being archived.		

Control ID	**AU-11(1)**	Control Name	**LONG-TERM RETRIEVAL CAPABILITY**
Definition	Employ [Assignment: organization-defined measures] to ensure that long-term audit records generated by the system can be retrieved.		
IHGIN Response	Audit records can be restored from archive at any time for a period of 7 years.		

Control ID	**AU-12**	Control Name	**Audit Record Generation**

Definition	a) Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components]; b) Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and c) Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.
IHGIN Response	Audit logs are generated system side and collected by our audit log collector. It is then analyzed by a SIEM solution to ensure that systems comply and are not experiencing any technical issues. The audit logs are generated in accordance with the IHGIN Security Policy.

Control ID	**AU-12(1)**	Control Name	**SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL**
Definition	Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].		
IHGIN Response	Audit records are compiled based upon the time provided by the NTP server. The time stamps tolerance is 5 minutes prior to network access being terminated. All systems are monitored for time shift monthly and restored to network time if required.		

Control ID	**AU-12(2)**	Control Name	**STANDARDIZED FORMATS**
Definition	Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.		
IHGIN Response	Audit logs are ingested into the collector and the SIEM solution will analyze them and maintain a standard format.		

Control ID	**AU-12(3)**	Control Name	**POLICY AND PROCEDURES**
Definition	Provide and implement the capability for [Assignment: organization-defined individuals or roles] to change the logging to be performed on [Assignment: organization-defined system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].		
IHGIN Response	Any time, there is a policy change or systems change the audit logging capabilities are reviewed and needs determined to best provide organizational security. These changes are then implemented by IT staff.		

Control ID	**AU-12(4)**	Control Name	**QUERY PARAMETER AUDITS OF PERSONALLY IDENTIFIABLE INFORMATION**
Definition	Provide and implement the capability for auditing the parameters of user query events for data sets containing personally identifiable information.		
IHGIN Response	Any query run on systems containing PII is logged and reviewed by our SIEM solution.		

Control ID	**AU-13**	Control Name	**Monitoring for Information Disclosure**
Definition	a) Monitor [Assignment: organization-defined open source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information; and b) If an information disclosure is discovered: 1. Notify [Assignment: organization-defined personnel or roles]; and 2. Take the following additional actions: [Assignment: organization-defined additional actions].		
IHGIN Response	Our email system monitors all outgoing communications for any information disclosure and will block outgoing emails if found to be in violation of the IHGIN Security Policy. The security appliance monitors all network traffic for information disclosure. The SIEM solution monitors both systems for any changes in behavior and provides an extra level of alerting to information sharing.		

Control ID	**AU-13(1)**	Control Name	**USE OF AUTOMATED TOOLS**
Definition	Monitor open source information and information sites using [Assignment: organization defined automated mechanisms].		
IHGIN Response	Monitoring of information and RSS feeds of security databases is conducted by IT staff to remain on-top of any new threats organizations are facing.		

Control ID	**AU-13(2)**	Control Name	**REVIEW OF MONITORED SITES**
Definition	Review the list of open source information sites being monitored [Assignment: organization-defined frequency].		
IHGIN Response	New sites are often added and monitored for information. Old sites are removed as information stops coming forward or become obsolete. We also monitor the darkweb for user database disclosures involving our email addresses.		

Control ID	**AU-13(3)**	Control Name	**UNAUTHORIZED REPLICATION OF INFORMATION**
Definition	Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.		
IHGIN Response	Data access to third parties is strictly controlled and monitored. Any replication that would be outside of the scope of the user or system is denied and flagged for review by IT staff.		

Control ID	**AU-14**	Control Name	**Session Audit**
Definition	a) Provide and implement the capability for [Assignment: organization-defined users or roles] to [Selection (one or more): record; view; hear; log] the content of a user session under [Assignment: organization-defined circumstances]; and b) Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.		
IHGIN Response	User sessions are logged in compliance with jurisdictional privacy laws, executive orders, directives, regulations, policies, standards, and guidelines.		

Control ID	**AU-14(1)**	Control Name	**SYSTEM START-UP**
Definition	Initiate session audits automatically at system start-up.		
IHGIN Response	Session audits begin at the time of system start-up.		

Control ID	**AU-14(2)**	Control Name	**CAPTURE AND RECORD CONTENT**
Definition	Deprecated (Implemented in AU-14)		
IHGIN Response	See response to AU-14		

Control ID	**AU-14(3)**	Control Name	**REMOTE VIEWING AND LISTENING**
Definition	Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.		
IHGIN Response	IT staff have the capability to view user's session and content in real-time on fixed systems. Mobile systems do not provide this functionality currently without rooting and due to the security concerns around third party rooting software this is not practiced by IT staff currently.		

Control ID	**AU-15**	Control Name	**Alternate Audit Logging Capability**
Definition	Deprecated (Implemented in AU-5(5))		
IHGIN Response	See response to AU-5(5)		

Control ID	**AU-16**	Control Name	**Cross-Organizational Audit Logging**
Definition	Employ [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.		
IHGIN Response	IHGIN does not ask third parties to provide audit logs of their systems nor provide third parties with access to audit logs. When information is transmitted into or out of the IHGIN network it is audited regardless of the source.		

Control ID	**AU-16(1)**	Control Name	**IDENTITY PRESERVATION**
Definition	Preserve the identity of individuals in cross-organizational audit trails.		
IHGIN Response	IHGIN does not ask third parties to provide audit logs of their systems nor provide third parties with access to audit logs. We do not conduct cross-organizational audit trails currently. This can be configured if required.		

Control ID	**AU-16(2)**	Control Name	**SHARING OF AUDIT INFORMATION**
Definition	Provide cross-organizational audit information to [Assignment: organization-defined organizations] based on [Assignment: organization-defined cross-organizational sharing agreements].		
IHGIN Response	IHGIN does not ask third parties to provide audit logs of their systems nor provide third parties with access to audit logs. We do not conduct cross-organizational audit		

	information sharing currently. This can be configured if required, but would need to be strictly controlled to protect the information of other customers.

Control ID	**AU-16(3)**	Control Name	**DISASSOCIABILITY**
Definition	Implement [Assignment: organization-defined measures] to disassociate individuals from audit information transmitted across organizational boundaries.		
IHGIN Response	IHGIN does not ask third parties to provide audit logs of their systems nor provide third parties with access to audit logs. The issue of disassociability is not applicable in this context.		

Assessment, Authorization, and Monitoring

Control ID	**CA-1**	Control Name	**POLICY AND PROCEDURES**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] assessment, authorization, and monitoring policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and c) Review and update the current assessment, authorization, and monitoring: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN lays out the policy being assessment, authorization, and monitoring within the IHGIN Security Policy. The policy addresses the purpose, scope, roles, and responsibilities of staff while reflecting management's commitment to ensuring that customer private information always remains private. All documentation is managed the organizational Enterprise Architect and the policies and procedures associated with this section are updated within the IHGIN Security Policy on a regular basis in response to systems change, regular review, or emerging threats.		

Control ID	**CA-2**	Control Name	**Control Assessments**
Definition	a) Develop a control assessment plan that describes the scope of the assessment including 1. Controls and control enhancements under assessment; 2. Assessment procedures to be used to determine control effectiveness; and		

	3. Assessment environment, assessment team, and assessment roles and responsibilities; b) Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment; c) Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements; d) Produce a control assessment report that document the results of the assessment; and e) Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].
IHGIN Response	IHGIN provides controls in-line with the IHGIN Security Policy that was developed using the NSIT 800-53 and CIS Controls V7. These security controls are reviewed on a regular basis and implemented or changed in accordance with the IHGIN Security Policy.

Control ID	**CA-2(1)**	Control Name	**INDEPENDENT ASSESSORS**
Definition	Employ independent assessors or assessment teams to conduct control assessments.		
IHGIN Response	Independent assessments of IHGIN IT systems and security is conducted and reported on to IHGIN management.		

Control ID	**CA-2(2)**	Control Name	**SPECIALIZED ASSESSMENTS**
Definition	Include as part of control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment [Assignment: organization-defined other forms of assessment]].		
IHGIN Response	Specialized assessments on systems are conducted when new systems are being implemented into the organization.		

Control ID	**CA-2(3)**	Control Name	**EXTERNAL ORGANIZATIONS**
Definition	Leverage the results of control assessments performed by [Assignment: organization defined external organization] on [Assignment: organization-defined system] when the assessment meets [Assignment: organization-defined requirements].		
IHGIN Response	Assessments done by third party organizations on systems deployed within the IHGIN environment are monitored for any security information disclosures and actions are taken to mitigate any risk associated with the disclosure.		

Control ID	**CA-3**	Control Name	**Information Exchange**
Definition	a) Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security		

	agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]]; b) Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and c) Review and update the agreements [Assignment: organization-defined frequency].
IHGIN Response	Prior to implementing any system that exchanges information externally, an agreement is entered into with the owner of the third-party system to ensure that information exchange is explicitly documented. The data exchange is reviewed to ensure that it still meets operational needs of all parties on a regular basis.

Control ID	**CA-3(1-5)**	Control Name	**Classification**
Definition	Deprecated (Implemented in SC-7(25-28,5)		
IHGIN Response	See response to SC7(25-28,5)		

Control ID	**CA-3(6)**	Control Name	**TRANSFER AUTHORIZATIONS**
Definition	Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.		
IHGIN Response	Third party systems are not allowed to initiate any connections into systems outside of the scope of the information exchange agreement.		

Control ID	**CA-3(7)**	Control Name	**TRANSITIVE INFORMATION EXCHANGES**
Definition	a) Identify transitive (downstream) information exchanges with other systems through the systems identified in CA-3a; and b) Take measures to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive (downstream) systems cannot be verified or validated.		
IHGIN Response	The SIEM solution monitors all information exchanges to ensure that is complies with organizational requirements. Downstream systems are prohibited from access to this information unless explicitly agreed to with the customers and the third party prior to implementation.		

Control ID	**CA-4**	Control Name	**Security Certification**
Definition	Deprecated (Implemented in CA-2)		
IHGIN Response	See response to CA-2		

Control ID	**CA-5**	Control Name	**Plan of Action and Milestones**

Definition	a) Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and b) Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, audits, and continuous monitoring activities.
IHGIN Response	IT maintains an organizational plan that outlines the timelines for implementation of key objectives and remediation actions to be taken to correct organizational weaknesses. The plan of action is updated quarterly to ensure that operational needs are being met and that all milestones are being achieved on target.

Control ID	**CA-5(1)**	Control Name	**AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY**
Definition	Ensure the accuracy, currency, and availability of the plan of action and milestones for the system using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	Automated tools are employed to help remind users of milestones and track the progress of the current tasks being completed by IT staff within the organization.		

Control ID	**CA-6**	Control Name	**Authorization**
Definition	a) Assign a senior official as the authorizing official for the system; b) Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems; c) Ensure that the authorizing official for the system, before commencing operations: 1. Accepts the use of common controls inherited by the system; and 2. Authorizes the system to operate; d) Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems; e) Update the authorizations [Assignment: organization-defined frequency].		
IHGIN Response	All controls and integration are authorized by the organizational Enterprise Architect who oversees all systems.		

Control ID	**CA-6(1)**	Control Name	**JOINT AUTHORIZATION — INTRA-ORGANIZATION**
Definition	Employ a joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization.		
IHGIN Response	The Enterprise Architect will report any control changes that impact users to the President and Vice President of the company to ensure that the impact can be managed. These controls require authorization from all parties to proceed.		

Control ID	**CA-6(2)**	Control Name	**JOINT AUTHORIZATION — INTER-ORGANIZATION**
Definition	Employ a joint authorization process for the system that includes multiple authorizing officials with at least one authorizing official from an organization external to the organization conducting the authorization.		

IHGIN Response	Control changes currently do not utilize a third party as part of the authorization process. Any customer facing changes or changes in controls that impact a customers data can be communicated with the customer for approval prior to implementation if required.

Control ID	**CA-7**	Control Name	**Continuous Monitoring**
Definition	a) Establishing the following system-level metrics to be monitored: [Assignment: organization defined system-level metrics]; b) Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness; c) Ongoing control assessments in accordance with the continuous monitoring strategy; d) Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy; e) Correlation and analysis of information generated by control assessments and monitoring; f) Response actions to address results of the analysis of control assessment and monitoring information; and g) Reporting the security and privacy status of the system to [Assignment: organization defined personnel or roles] [Assignment: organization-defined frequency].		
IHGIN Response	All systems are continuously monitored to ensure that operational needs are met. The SIEM solution provides monitoring and analysis for the organization to ensure that we meet the objectives of CA-7.		

Control ID	**CA-7(1)**	Control Name	**INDEPENDENT ASSESSMENT**
Definition	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.		
IHGIN Response	Independent audits are conducted on systems by third party assessors as required. These audits look at controls and ensure they are meeting the requirements and needs of the business.		

Control ID	**CA-7(2)**	Control Name	**TYPES OF ASSESSMENTS**
Definition	Deprecated (Incorporated in CA-2)		
IHGIN Response	See response to CA-2		

Control ID	**CA-7(3)**	Control Name	**TREND ANALYSES**
Definition	Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.		
IHGIN Response	The IHGIN SIEM solution and adaptive threat protection provide trend analysis to protect against emerging threats.		

Control ID	**CA-7(4)**	Control Name	**RISK MONITORING**
Definition	Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following: a) Effectiveness monitoring; b) Compliance monitoring; and c) Change monitoring.		
IHGIN Response	IT staff evaluate risk on an ongoing basis an re-evaluate risks semi-annually or whenever a technological change is introduced to ensure that the organization isn't taking an undue risk. Additionally all systems are monitored for potential risk exposure using our vulnerability analysis suite on a regular basis.		

Control ID	**CA-7(5)**	Control Name	**CONSISTENCY ANALYSIS**
Definition	Employ the following actions to validate that policies are established and implemented controls are operating in a consistent manner: [Assignment: organization-defined actions].		
IHGIN Response	The SIEM solution will alert if a system is acting outside of the baseline.		

Control ID	**CA-8**	Control Name	**Penetration Testing**
Definition	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].		
IHGIN Response	A penetration test of systems is conducted as needed without IT staff awareness to ensure the penetration test shows real-world response to active threats by a third party.		

Control ID	**CA-8(1)**	Control Name	**INDEPENDENT PENETRATION TESTING AGENT OR TEAM**
Definition	Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.		
IHGIN Response	A penetration test of systems is conducted as needed without IT staff awareness to ensure the penetration test shows real-world response to active threats by a third party.		

Control ID	**CA-8(2)**	Control Name	**RED TEAM EXERCISES**
Definition	Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises].		
IHGIN Response	Red team exercises are conducted without IT staff awareness to test real work response. The rules of engagement are outlined ahead of time as to not cause any disruption to IT operations.		

Control ID	**CA-8(3)**	Control Name	**FACILITY PENETRATION TESTING**

Definition	Employ a penetration testing process that includes [Assignment: organization-defined frequency] [Selection: announced; unannounced] attempts to bypass or circumvent controls associated with physical access points to the facility
IHGIN Response	A penetration test of systems is conducted as needed without IT staff awareness to ensure the penetration test shows real-world response to active threats by a third party.

Control ID	**CA-9**	Control Name	**Internal System Connections**
Definition	a) Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system; b) Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated; c) Terminate internal system connections after [Assignment: organization-defined conditions]; and d) Review [Assignment: organization-defined frequency] the continued need for each internal connection.		
IHGIN Response	Internal connections between different security domains is routed through our firewall, and only information allowed between the networks is passed. The information is scanned while in transit between the networks to ensure that the traffic does not match known attack patterns. Any networked triggered events are logged and analyzed by our SIEM solution in near real-time. Connections between networks has a designated TTL to ensure that connections don't remain open.		

Control ID	**CA-9(1)**	Control Name	**COMPLIANCE CHECKS**
Definition	Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.		
IHGIN Response	The SIEM solution and vulnerability analysis suite allows IHGIN to ensure that compliance is being maintained. Reports are generated to show that systems are in compliance, and IT will investigate systems manually and test them to ensure that the baseline for each system is correct.		

Configuration Management

Control ID	**CM-1**	Control Name	**POLICY AND PROCEDURES**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] configuration management policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;		

	b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and c) Review and update the current configuration management: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	Configurations are created and maintained by IHGIN IT staff in-line with the IHGIN Security Policy. Configuration changes are done based upon business need and tested by IT staff prior to being implemented. Configuration files are monitored for changes and IT staff ensure that changes made are reviewed prior to implementation.

Control ID	**CM-2**	Control Name	**Baseline Configuration**
Definition	a) Develop, document, and maintain under configuration control, a current baseline configuration of the system; and b) Review and update the baseline configuration of the system: 1. [Assignment: organization-defined frequency]; 2. When required due to [Assignment organization-defined circumstances]; and 3. When system components are installed or upgraded.		
IHGIN Response	A baseline configuration of a system is established prior to implementation. Any changes to this baseline are reviewed internally and tested. The configuration baseline is established in the SIEM solution and monitored to ensure that system is not changed without IT review.		

Control ID	**CM-2(1)**	Control Name	**REVIEWS AND UPDATES**
Definition	Deprecated (Implemented in CM-2)		
IHGIN Response	See response to CM-2		

Control ID	**CM-2(2)**	Control Name	**AUTOMATION SUPPORT FOR ACCURACY AND CURRENCY**
Definition	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	Internal tools are used to automatically track firmware version numbers, applications installed, patches applied, and configurations. Changes to these systems are monitored by the SIEM solution and reported to IT staff. Additionally IHGIN conducts routine vulnerability scans against these systems to ensure that important security patches are applied to all systems.		

Control ID	**CM-2(3)**	Control Name	**RETENTION OF PREVIOUS CONFIGURATIONS**
Definition	Retain [Assignment: organization-defined number] of previous versions of baseline configurations of the system to support rollback.		

IHGIN Response	Previous versions of configurations are stored on backup for restoration in the case that a patch or configuration change causes issues. Where applicable, a snapshot is taken prior to the change being implemented.

Control ID	**CM-2(4)**	Control Name	**UNAUTHORIZED SOFTWARE**
Definition	Deprecated (Implemented in CM-7(4))		
IHGIN Response	See response to CM-7(4)		

Control ID	**CM-2(5)**	Control Name	**AUTHORIZED SOFTWARE**
Definition	Deprecated (Implemented in CM-7(5))		
IHGIN Response	See response to CM-7(5)		

Control ID	**CM-2(6)**	Control Name	**DEVELOPMENT AND TEST ENVIRONMENTS**
Definition	Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.		
IHGIN Response	The development and test environment has a separate operational baseline configuration than production. Though it mirrors production where applicable.		

Control ID	**CM-2(7)**	Control Name	**CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS**
Definition	a) Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and b) Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls].		
IHGIN Response	Systems that are used for travel or outside of the organization have strict controls applied to them under the IHGIN security policy. This includes encryption methodologies, VPN access, and rules around wireless network usage. Additional software is installed on these devices to closely monitor them while being utilized in the field.		

Control ID	**CM-3**	Control Name	**Configuration Change Control**
Definition	a) Determine and document the types of changes to the system that are configuration controlled; b) Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses; c) Document configuration change decisions associated with the system; d) Implement approved configuration-controlled changes to the system; e) Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time-period];		

	f) Monitor and review activities associated with configuration-controlled changes to the system; and g) Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].
IHGIN Response	All changes to systems configuration are documented and controlled by IHGIN IT staff. Changes to key systems are reviewed prior to implementation and approved by IT management. A risk assessment, along with an impact analysis is done to determine the overall scope of the change. Any change that is implemented is closely monitored and reviewed to ensure that no unintended consequences emerge from the change.

Control ID	**CM-3(1)**	Control Name	**AUTOMATED DOCUMENTATION, NOTIFICATION, AND PROHIBITION OF CHANGES**
Definition	Use [Assignment: organization-defined automated mechanisms] to: a) Document proposed changes to the system; b) Notify [Assignment: organization-defined approval authorities] of proposed changes to the system and request change approval; c) Highlight proposed changes to the system that have not been approved or disapproved within [Assignment: organization-defined time-period]; d) Prohibit changes to the system until designated approvals are received; e) Document all changes to the system; and f) Notify [Assignment: organization-defined personnel] when approved changes to the system are completed.		
IHGIN Response	Change management is a manual process currently at IHGIN. A few systems will generate documentation or emails upon changes being implemented. All changes are reviewed by IHGIN IT staff and document prior to rollout and monitored closely after implementation.		

Control ID	**CM-3(2)**	Control Name	**TESTING, VALIDATION, AND DOCUMENTATION OF CHANGES**
Definition	Test, validate, and document changes to the system before finalizing the implementation of the changes		
IHGIN Response	All systems changes are tested for functionality and validated prior to implementation. Changes are documented and monitored to ensure that no unintended consequences emerge from the change.		

Control ID	**CM-3(3)**	Control Name	**AUTOMATED CHANGE IMPLEMENTATION**
Definition	Implement changes to the current system baseline and deploy the updated baseline across the installed base using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	Our SIEM solution will automatically notify of changes that have been implemented to systems and monitor all systems for changes to baselined information.		

Control ID	**CM-3(4)**	Control Name	**SECURITY AND PRIVACY REPRESENTATIVES**
Definition	Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].		
IHGIN Response	IHGIN IT staff are trained on systems security procedures and controls. The Enterprise Architect has significant experience and qualifications in IT security and privacy. All changes to infrastructure are reviewed prior to implementation by the Enterprise Architect to ensure that unintended consequences are minimalized.		

Control ID	**CM-3(5)**	Control Name	**AUTOMATED SECURITY RESPONSE**
Definition	Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner: [Assignment: organization-defined security responses].		
IHGIN Response	The SIEM solution will automatically flag configuration changes for review and can take automated action to block systems access if the change is determined by analysis to be malicious.		

Control ID	**CM-3(6)**	Control Name	**CRYPTOGRAPHY MANAGEMENT**
Definition	Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [Assignment: organization-defined controls].		
IHGIN Response	IHGIN IT staff are responsible for ensuring that cryptographic items such as certificates are managed and updated prior to expiration and that all cryptographic methods remain up to date.		

Control ID	**CM-3(7)**	Control Name	**REVIEW SYSTEM CHANGES**
Definition	Review changes to the system [Assignment: organization-defined frequency] or when [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.		
IHGIN Response	Systems changes are reviewed on a regular basis to ensure that configuration items did not get overlooked. Systems are scanned for vulnerabilities to software and configurations to ensure that best practices have been implemented across the environment.		

Control ID	**CM-3(8)**	Control Name	**PREVENT OR RESTRICT CONFIGURATION CHANGES**
Definition	Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].		
IHGIN Response	Only IT staff have the capability to make configuration changes within the environment and privileged accounts are strictly controlled.		

Control ID	**CM-4**	Control Name	**Impact Analyses**
Definition	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.		

IHGIN Response	Prior to implementation of any systems change, the Enterprise Architect will conduct an impact analyses to ensure that all systems remain secure and operational.

Control ID	**CM-4(1)**	Control Name	**SEPARATE TEST ENVIRONMENTS**
Definition	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.		
IHGIN Response	The test environment is used to conduct testing on configuration changes prior to implementation into the production environment.		

Control ID	**CM-4(2)**	Control Name	**VERIFICATION OF CONTROLS**
Definition	After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.		
IHGIN Response	Controls are verified using the SIEM solution and using vulnerability scanning and assessments. Additionally penetration tests and red team exercises are conducted in an ad-hoc fashion to ensure that controls are functioning as intended.		

Control ID	**CM-5**	Control Name	**Access Restrictions for Change**
Definition	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.		
IHGIN Response	Physical and logical access restrictions are in place to ensure that only approved personnel have access to make changes.		

Control ID	**CM-5(1)**	Control Name	**AUTOMATED ACCESS ENFORCEMENT AND AUDIT RECORDS**
Definition	a) Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and b) Automatically generate audit records of the enforcement actions.		
IHGIN Response	Changes to configuration and account log-on events associated with the changes are logged and analyzed by the SIEM solution. The audit records of these changes along with all other changes are maintained according to the IHGIN Security Policy.		

Control ID	**CM-5(2)**	Control Name	**REVIEW SYSTEM CHANGES**
Definition	Deprecated (Implemented in CM-3(7))		
IHGIN Response	See response to CM-3(7)		

Control ID	**CM-5(3)**	Control Name	**SIGNED COMPONENTS**
Definition	Prevent the installation of [Assignment: organization-defined software and firmware components] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.		

IHGIN Response	At this time IHGIN does not require signed components for software being installed on systems. Instead we require that the software come from a known vendor and is tested prior to implementation. The requirement for signed components can be implemented if required.

Control ID	**CM-5(4)**	Control Name	**DUAL AUTHORIZATION**
Definition	Enforce dual authorization for implementing changes to [Assignment: organization defined system components and system-level information].		
IHGIN Response	Currently IHGIN does not require dual authorization for the implementation of systems changes. Instead IHGIN requires systems changes be tested, verified, and approved by the Enterprise Architect prior to implementation.		

Control ID	**CM-5(5)**	Control Name	**PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION**
Definition	a) Limit privileges to change system components and system-related information within a production or operational environment; and b) Review and reevaluate privileges [Assignment: organization-defined frequency].		
IHGIN Response	Privileges to make changes to the environment and systems is prohibited to IT staff under strict control.		

Control ID	**CM-6(6)**	Control Name	**LIMIT LIBRARY PRIVILEGES**
Definition	Limit privileges to change software resident within software libraries.		
IHGIN Response	This privilege is limited to IT staff.		

Control ID	**CM-5(7)**	Control Name	**AUTOMATIC IMPLEMENTATION OF SECURITY SAFEGUARDS**
Definition	Deprecated (Implemented in SI-7)		
IHGIN Response	See response to SI-7		

Control ID	**CM-6**	Control Name	**Configuration Settings**
Definition	a) Establish and document configuration settings for components employed within the system using [Assignment: organization-defined common secure configurations] that reflect the most restrictive mode consistent with operational requirements; b) Implement the configuration settings; c) Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization defined operational requirements]; and d) Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.		

IHGIN Response	Configuration documentation is maintained by IHGIN IT staff. Configurations and patch management is outlined for both hardware and software by IT operational policies. Configurations are monitored by the SIEM solution to ensure that they do not deviate from established settings and systems are scanned to ensure that standard configurations remain secure as new exploits are found and released.

Control ID	**CM-6(1)**	Control Name	**AUTOMATED MANAGEMENT, APPLICATION, AND VERIFICATION**
Definition	Centrally manage, apply, and verify configuration settings for [Assignment: organization defined system components] using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	Configuration settings are remotely monitored using the SIEM solution and verified in real-time to ensure that they do not deviate from the baseline.		

Control ID	**CM-6(2)**	Control Name	**RESPOND TO UNAUTHORIZED CHANGES**
Definition	Take the following actions in response to unauthorized changes to [Assignment: organization-defined configuration settings]: [Assignment: organization-defined actions].		
IHGIN Response	If an unauthorized change to a system is detected by the SIEM solution, IT staff are alerted in real-time. IT can then isolate the machine and test the configuration to determine the root cause of the unauthorized change.		

Control ID	**CM-6(3)**	Control Name	**UNAUTHORIZED CHANGE DETECTION**
Definition	Deprecated (Implemented in SI-7)		
IHGIN Response	See response to SI-7		

Control ID	**CM-6(4)**	Control Name	**CONFORMANCE DEMONSTRATION**
Definition	Deprecated (Implemented in CM-4)		
IHGIN Response	See response to CM-4		

Control ID	**CM-7**	Control Name	**Least Functionality**
Definition	a) Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and b) Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, software, and/or services].		
IHGIN Response	IT systems are configured to meet the business functions they are designed to meet. They provide only the services required and nothing else. Installing extra services and software onto production servers is strictly prohibited. IHGIN IT has a test environment to conduct any activities that may not meet the principle of least functionality.		

Control ID	**CM-7(1)**	Control Name	**PERIODIC REVIEW**
Definition	a) Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and b) Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].		
IHGIN Response	IHGIN IT will review systems for functional states on a regular basis and disable/remove software and services that are no longer providing business value or that may present unnecessary risk.		

Control ID	**CM-7(2)**	Control Name	**PREVENT PROGRAM EXECUTION**
Definition	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].		
IHGIN Response	IT staff control the installation of programs on machines and will only install applications that have met the defined needs of the user. The installation and usage of unauthorized programs is prohibited.		

Control ID	**CM-7(3)**	Control Name	**REGISTRATION COMPLIANCE**
Definition	Ensure compliance with [Assignment: organization-defined registration requirements for functions, ports, protocols, and services].		
IHGIN Response	The SIEM solution and enterprise network security solution both register ports, protocols, and services management within their respective systems and monitor for compliance.		

Control ID	**CM-7(4)**	Control Name	**UNAUTHORIZED SOFTWARE — BLACKLISTING**
Definition	a) Identify [Assignment: organization-defined software programs not authorized to execute on the system]; b) Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and c) Review and update the list of unauthorized software programs [Assignment: organization-defined frequency].		
IHGIN Response	Specific file types are blacklisted by IT from being used within the organization. Software not approved by IT is considered blacklisted by default.		

Control ID	**CM-7(5)**	Control Name	**AUTHORIZED SOFTWARE — WHITELISTING**
Definition	a) Identify [Assignment: organization-defined software programs authorized to execute on the system]; b) Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and c) Review and update the list of authorized software programs [Assignment: organization-defined frequency].		

IHGIN Response	IT maintains a list of approved software for use within the enterprise. This software list is reviewed on a regular basis and updated with approved versions. Occasionally software is removed and added to the authorized list depending on business need or security concern.

Control ID	**CM-7(6)**	Control Name	**CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES**
Definition	Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user installed software].		
IHGIN Response	IT maintains a test environment that is isolated from the production systems for testing software or executing code that has not been approved for production.		

Control ID	**CM-7(7)**	Control Name	**CODE EXECUTION IN PROTECTED ENVIRONMENTS**
Definition	Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of [Assignment: organization defined personnel or roles] when such code is: a) Obtained from sources with limited or no warranty; and/or b) Without the provision of source code.		
IHGIN Response	IT maintains a test environment that is isolated from the production systems for testing software or executing code that has not been approved for production.		

Control ID	**CM-7(8)**	Control Name	**BINARY OR MACHINE EXECUTABLE CODE**
Definition	a) Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; and b) Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.		
IHGIN Response	IT maintains a test environment that is isolated from the production systems for testing software or executing code that has not been approved for production. Once tested and confirmed to be safe and meet organizational need the program or code may be moved into production to serve the business function as required with the approval of the Enterprise Architect.		

Control ID	**CM-8**	Control Name	**System Component Inventory**
Definition	a) Develop and document an inventory of system components that: 1. Accurately reflects the system; 2. Includes all components within the system; 3. Is at the level of granularity deemed necessary for tracking and reporting; and 4. Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and b) Review and update the system component inventory [Assignment: organization-defined frequency].		

IHGIN Response	IT maintains an inventory of assets and system components. This is reviewed annually and maintained on an ongoing basis.

Control ID	**CM-8(1)**	Control Name	**UPDATES DURING INSTALLATION AND REMOVAL**
Definition	Update the inventory of system components as part of component installations, removals, and system updates.		
IHGIN Response	When systems are updated with new components or anytime a new component is added to the environment the inventory is updated to reflect the change.		

Control ID	**CM-8(2)**	Control Name	**AUTOMATED MAINTENANCE**
Definition	Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	Automated scans are conducted to ensure that systems components are not changed without authorization.		

Control ID	**CM-8(3)**	Control Name	**AUTOMATED UNAUTHORIZED COMPONENT DETECTION**
Definition	a) Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; and b) Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].		
IHGIN Response	Automated scans are conducted to ensure that systems components are not changed without authorization. Any unauthorized systems are isolated automatically until IT approves the device for usage.		

Control ID	**CM-8(4)**	Control Name	**ACCOUNTABILITY INFORMATION**
Definition	Include in the system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible and accountable for administering those components.		
IHGIN Response	The systems administrator is responsible for ensuring the inventory of assets is updated and maintained.		

Control ID	**CM-8(5)**	Control Name	**NO DUPLICATE ACCOUNTING OF COMPONENTS**
Definition	a) Verify that all components within the system are not duplicated in other system component inventories; or b) If a centralized component inventory is used, verify components are not assigned to multiple systems.		
IHGIN Response	Serial numbers and mac addresses are used to ensure that duplicate components are not logged in the inventory.		

Control ID	**CM-8(6)**	Control Name	**ASSESSED CONFIGURATIONS AND APPROVED DEVIATIONS**

Definition	Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.
IHGIN Response	Configuration and systems changes are monitored by our SIEM solution to ensure that new components or configuration changes are flagged for approval.

Control ID	**CM-8(7)**	Control Name	**CENTRALIZED REPOSITORY**
Definition	Provide a centralized repository for the inventory of system components		
IHGIN Response	IT maintains a centralized repository that houses an inventory of all systems and components.		

Control ID	**CM-8(8)**	Control Name	**AUTOMATED LOCATION TRACKING**
Definition	Support the tracking of system components by geographic location using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	Remote assets are tracked using our mobile device management solution using geographic location services. The inventory database maintains a list of where systems are located. Moving of system is conducted by IT staff and as procedure the inventory database is to be updated when systems are moved.		

Control ID	**CM-8(9)**	Control Name	**ASSIGNMENT OF COMPONENTS TO SYSTEMS**
Definition	a) Assign [Assignment: organization-defined acquired system components] to a system; and b) Receive an acknowledgement from [Assignment: organization-defined personnel or roles] of this assignment		
IHGIN Response	Components are assigned to systems and tickets are updated to show when they have been configured/installed in said system.		

Control ID	**CM-9**	Control Name	**Configuration Management Plan**
Definition	Develop, document, and implement a configuration management plan for the system that: a) Addresses roles, responsibilities, and configuration management processes and procedures; b) Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; c) Defines the configuration items for the system and places the configuration items under configuration management; d) Is reviewed and approved by [Assignment: organization-defined personnel or roles]; and e) Protects the configuration management plan from unauthorized disclosure and modification.		
IHGIN Response	IHGIN enterprise architect reviews all systems and maintains a configuration plan and documents each specific system as far as business need/value and configuration implemented to meet that need.		

Control ID	**CM-9(1)**	Control Name	**ASSIGNMENT OF RESPONSIBILITY**
Definition	Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.		
IHGIN Response	IT staff are responsible for maintaining the configuration management process.		

Control ID	**CM-10**	Control Name	**Software Usage Restrictions**
Definition	a) Use software and associated documentation in accordance with contract agreements and copyright laws; b) Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and c) Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.		
IHGIN Response	Software use is tracked by the SIEM solution, and software installation is controlled by IT staff. End users are not allowed to install software onto their computers without IT intervention. Peer-to-Peer file sharing and known pirate software sites and blocked at the firewall level.		

Control ID	**CM-10(1)**	Control Name	**OPEN SOURCE SOFTWARE**
Definition	Establish the following restrictions on the use of open source software: [Assignment: organization-defined restrictions].		
IHGIN Response	Open-source software is only allowed from approved sources by the IT department. Open-source software follows a separate patch management strategy than closed-source solutions and is monitored for vulnerabilities using our vulnerability scanner and monitored against a usage baseline established within our SIEM solution.		

Control ID	**CM-11**	Control Name	**User-Installed Software**
Definition	a) Establish [Assignment: organization-defined policies] governing the installation of software by users; b) Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and c) Monitor policy compliance [Assignment: organization-defined frequency].		
IHGIN Response	Users are prohibited from installing software. Compliance with this policy is monitored by the SIEM solution.		

Control ID	**CM-11(1)**	Control Name	**ALERTS FOR UNAUTHORIZED INSTALLATIONS**
Definition	Deprecated (Implemented in CM-8(3))		
IHGIN Response	See response to CM-8(3)		

Control ID	**CM-11(2)**	Control Name	**SOFTWARE INSTALLATION WITH PRIVILEGED STATUS**
Definition	Allow user installation of software only with explicit privileged status		

IHGIN Response	Only IT Staff with privileged domain accounts or LAPS are allowed to install software on local machines.

Control ID	**CM-12**	Control Name	**Information Location**
Definition	a) Identify and document the location of [Assignment: organization-defined information] and the specific system components on which the information is processed and stored; b) Identify and document the users who have access to the system and system components where the information is processed and stored; and c) Document changes to the location (i.e., system or system components) where the information is processed and stored.		
IHGIN Response	The location of information is documented along with the users that have access to said information. Changes to locations are reflected in documentation at the time of change.		

Control ID	**CM-12(1)**	Control Name	**AUTOMATED TOOLS TO SUPPORT INFORMATION LOCATION**
Definition	Use automated tools to identify [Assignment: organization-defined information by information type] on [Assignment: organization-defined system components] to ensure controls are in place to protect organizational information and individual privacy.		
IHGIN Response	Auditing is enabled data storage locations to monitor for any changes in location. This is reflected in the SIEM solution.		

Control ID	**CM-13**	Control Name	**Data Action Mapping**
Definition	Develop and document a map of system data actions		
IHGIN Response	Any system that processes PII has a data-map created to show the flow of data and actions taken by the system on that data.		

Contingency Planning

Control ID	**CP-1**	Control Name	**POLICY AND PROCEDURES**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] contingency planning policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;		

	b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and c) Review and update the current contingency planning: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	Contingency planning is established in the disaster recover plan and risk management plan for each project undertaken by IHGIN IT.

Control ID	**CP-2**	Control Name	**Contingency Plan**
Definition	a) Develop a contingency plan for the system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite a system disruption, compromise, or failure; 5. Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b) Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c) Coordinate contingency planning activities with incident handling activities; d) Review the contingency plan for the system [Assignment: organization-defined frequency]; e) Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f) Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g) Protect the contingency plan from unauthorized disclosure and modification.		
IHGIN Response	IHGIN ensures that the disaster recovery plan takes into consideration all items within CP-2. The disaster recovery plan is updated and tested on a regular basis. It is prohibited from being shared outside of the organization without management approval.		

Control ID	**CP-2(1)**	Control Name	**COORDINATE WITH RELATED PLANS**
Definition	Coordinate contingency plan development with organizational elements responsible for related plans.		
IHGIN Response	Related business continuity plans for each department are coordinated with the disaster recovery plan to ensure operation needs and priorities are established to provide the best service to IHGIN customers.		

Control ID	**CP-2(2)**	Control Name	**CAPACITY PLANNING**
Definition	Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.		
IHGIN Response	IHGIN IT has ensured that back-up systems and disaster recovery systems meet capacity needs for the organization in a disaster situation.		

Control ID	**CP-2(3)**	Control Name	**RESUME MISSIONS AND BUSINESS FUNCTIONS**
Definition	Plan for the resumption of [Selection: all; essential] missions and business functions within [Assignment: organization-defined time-period] of contingency plan activation.		
IHGIN Response	The disaster recovery plan highlights the requirements for a resumption of business operations.		

Control ID	**CP-2(4)**	Control Name	**RESUME ALL MISSIONS AND BUSINESS FUNCTIONS**
Definition	Deprecated (Implemented in CP-2(3))		
IHGIN Response	See response to CP-2(3)		

Control ID	**CP-2(5)**	Control Name	**CONTINUE MISSIONS AND BUSINESS FUNCTIONS**
Definition	Plan for the continuance of [Selection: all; essential] missions and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.		
IHGIN Response	IHGIN disaster recovery plan outlines how the organization can continue the missions and business functions in a disaster event.		

Control ID	**CP-2(6)**	Control Name	**ALTERNATE PROCESSING AND STORAGE SITES**
Definition	Plan for the transfer of [Selection: all; essential] missions and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.		
IHGIN Response	IHGIN has outlined the alternate locations for processing and storage in the disaster recovery plan.		

Control ID	**CP-2(7)**	Control Name	**COORDINATE WITH EXTERNAL SERVICE PROVIDERS**
Definition	Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.		
IHGIN Response	IHGIN has contacted suppliers to ensure that backup materials, supplies, and equipment can be procured prior to backup supply running out.		

Control ID	**CP-2(8)**	Control Name	**IDENTIFY CRITICAL ASSETS**
Definition	Identify critical system assets supporting [Selection: all; essential] missions and business functions.		

IHGIN Response	Critical assets have been identified and organizational redundancy created to ensure business operations are not interrupted.

Control ID	**CP-3**	Control Name	**Contingency Training**
Definition	Provide contingency training to system users consistent with assigned roles and responsibilities: a) Within [Assignment: organization-defined time-period] of assuming a contingency role or responsibility; b) When required by system changes; and c) [Assignment: organization-defined frequency] thereafter		
IHGIN Response	Users are required to review and participate in training on business continuity and disaster recovery.		

Control ID	**CP-3(1)**	Control Name	**SIMULATED EVENTS**
Definition	Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.		
IHGIN Response	IHGIN simulates a disaster event to ensure staff know their role in a crisis.		

Control ID	**CP-3(2)**	Control Name	**MECHANISMS USED IN TRAINING ENVIRONMENTS**
Definition	Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.		
IHGIN Response	IHGIN IT fully tests the disaster recovery plan on an annual basis in a real-world scenario.		

Control ID	**CP-4**	Control Name	**Contingency Plan Testing**
Definition	a) Test the contingency plan for the system [Assignment: organization-defined frequency] using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: [Assignment: organization-defined tests]. b) Review the contingency plan test results; and c) Initiate corrective actions, if needed.		
IHGIN Response	After each test of the disaster recovery plan, the plan is reviewed for potential weaknesses and updated.		

Control ID	**CP-4(1)**	Control Name	**COORDINATE WITH RELATED PLANS**
Definition	Coordinate contingency plan testing with organizational elements responsible for related plans.		
IHGIN Response	All related plans are updated with each test of the disaster recover plan.		

Control ID	**CP-4(2)**	Control Name	**ALTERNATE PROCESSING SITE**
Definition	Test the contingency plan at the alternate processing site:		

	a) To familiarize contingency personnel with the facility and available resources; and b) To evaluate the capabilities of the alternate processing site to support contingency operations.
IHGIN Response	IHGIN maintains a geographically redundant alternate processing site. The site has the built-in capacity to take-over operations as needed in a disaster event.

Control ID	**CP-4(3)**	Control Name	**AUTOMATED TESTING**
Definition	Test the contingency plan using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	IHGIN internal systems are stress tested during the disaster recovery scenario to simulate real-world traffic. This automated test ensures that systems are not only operation, but can actually meet the demands of service without degradation.		

Control ID	**CP-4(4)**	Control Name	**FULL RECOVERY AND RECONSTITUTION**
Definition	Include a full recovery and reconstitution of the system to a known state as part of contingency plan testing.		
IHGIN Response	The full recovery and reconstitution of systems to a known state is part of our disaster recovery plan testing.		

Control ID	**CP-5**	Control Name	**Contingency Plan Update**
Definition	Deprecated (Implemented in CP-2)		
IHGIN Response	See response to CP-2		

Control ID	**CP-6**	Control Name	**Alternate Storage Site**
Definition	a) Establish an alternate storage site, including necessary agreements to permit the storage and retrieval of system backup information; and b) Ensure that the alternate storage site provides controls equivalent to that of the primary site		
IHGIN Response	An alternate storage site with equivalent physical security controls has been established in a geographically redundant location.		

Control ID	**CP-6(1)**	Control Name	**SEPARATION FROM PRIMARY SITE**
Definition	Identify an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats.		
IHGIN Response	An alternate storage site with equivalent physical security controls has been established in a geographically redundant location.		

Control ID	**CP-6(2)**	Control Name	**RECOVERY TIME AND RECOVERY POINT OBJECTIVES**
Definition	Configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.		

IHGIN Response	The alternate storage site is a fully operational plan in a geographically redundant location capable of taking on the additional capacity.

Control ID	**CP-6(3)**	Control Name	**ACCESSIBILITY**
Definition	Identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.		
IHGIN Response	An alternate storage site with equivalent physical security controls has been established in a geographically redundant location. The site is located over 1000 miles away. Accessibility to the alternate location should not be disrupted by a disaster to the IHGIN facility. In the case that it is, IHGIN can shift to a third site located in another geographically redundant location.		

Control ID	**CP-7**	Control Name	**Alternate Processing Site**
Definition	a) Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential missions and business functions within [Assignment: organization-defined time-period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable; b) Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time-period for transfer and resumption; and c) Provide controls at the alternate processing site that are equivalent to those at the primary site.		
IHGIN Response	IHGIN maintains an alternate processing facility in Amherst, Nova Scotia, Canada that can facilitate full operations if required in a disaster situation. All controls provided at the IHGIN facility exist at the Amherst facility and the equipment and materials required to continue operations are maintained in duplicate.		

Control ID	**CP-7(1)**	Control Name	**SEPARATION FROM PRIMARY SITE**
Definition	Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.		
IHGIN Response	IHGIN maintains an alternate processing facility in Amherst, Nova Scotia, Canada that is over 1000 miles away from the IHGIN facility.		

Control ID	**CP-7(2)**	Control Name	**ACCESSIBILITY**
Definition	Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.		
IHGIN Response	The alternate processing facility is over 1000 miles away, it should not be impacted by an area-wide disruption or disaster. In the case that it is, IHGIN can shift production to a third site located in Quebec Canada.		

Control ID	**CP-7(3)**	Control Name	**PRIORITY OF SERVICE**

Definition	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).
IHGIN Response	IHGIN maintains a recovery time objective of 24 hours for operations to shift to the alternate processing site.

Control ID	**CP-7(4)**	Control Name	**PREPARATION FOR USE**
Definition	Prepare the alternate processing site so that the site can serve as the operational site supporting essential missions and business functions.		
IHGIN Response	The alternate site processes millions of license plates per year currently. Shifting essential business functions to the alternate site can easily be done by IHGIN in the case of a disaster.		

Control ID	**CP-7(5)**	Control Name	**EQUIVALENT INFORMATION SECURITY SAFEGUARDS**
Definition	Deprecated (Implemented in CP-7)		
IHGIN Response	See response to CP-7		

Control ID	**CP-7(6)**	Control Name	**INABILITY TO RETURN TO PRIMARY SITE**
Definition	Plan and prepare for circumstances that preclude returning to the primary processing site.		
IHGIN Response	IHGIN can continue operations at the back-up facility until a new primary site has been established and tested.		

Control ID	**CP-8**	Control Name	**Telecommunications Services**
Definition	Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential missions and business functions within [Assignment: organization-defined time-period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.		
IHGIN Response	IHGIN maintains the ability to switch between ISPs to maintain business operations.		

Control ID	**CP-8(1)**	Control Name	**PRIORITY OF SERVICE PROVISIONS**
Definition	a) Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and b) Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier		
IHGIN Response	IHGIN has agreements with their ISP to meet availability requirements. Backup communications are maintained using an alternate peering provider to ensure operational continuance in the case of a national telecommunications outage.		

Control ID	**CP-8(2)**	Control Name	**SINGLE POINTS OF FAILURE**
Definition	Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.		
IHGIN Response	IHGIN currently maintains only one ISP but has an alternate backup ISP identified for installation if needed. If required, IHGIN can maintain a hot backup for internet connectivity.		

Control ID	**CP-8(3)**	Control Name	**SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS**
Definition	Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.		
IHGIN Response	IHGIN currently maintains only one ISP but has an alternate backup ISP identified for installation if needed. If required, IHGIN can maintain a hot backup for internet connectivity.		

Control ID	**CP-8(4)**	Control Name	**PROVIDER CONTINGENCY PLAN**
Definition	a) Require primary and alternate telecommunications service providers to have contingency plans; b) Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and c) Obtain evidence of contingency testing and training by providers [Assignment: organization-defined frequency].		
IHGIN Response	ISP providers are required to have appropriate contingency plans.		

Control ID	**CP-8(5)**	Control Name	**ALTERNATE TELECOMMUNICATION SERVICE TESTING**
Definition	Test alternate telecommunication services [Assignment: organization-defined frequency].		
IHGIN Response	Alternate telecommunications equipment and services are tested on an on-going basis.		

Control ID	**CP-9**	Control Name	**System Backup**
Definition	a) Conduct backups of user-level information contained in [Assignment: organization-defined system components] [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; b) Conduct backups of system-level information contained in the system [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; c) Conduct backups of system documentation, including security and privacy-related documentation [Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]; and d) Protect the confidentiality, integrity, and availability of backup information		

IHGIN Response	Systems backups take place on-site and off-site nightly. The on-site backups are encrypted at rest, and the cloud-based backup and recovery is encrypted in transit and at rest. These backups are monitored to ensure they are always operational.

Control ID	**CP-9(1)**	Control Name	**TESTING FOR RELIABILITY AND INTEGRITY**
Definition	Test backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.		
IHGIN Response	Backups are fully tested as part of the IT disaster recovery plan and security policy.		

Control ID	**CP-9(2)**	Control Name	**TEST RESTORATION USING SAMPLING**
Definition	Use a sample of backup information in the restoration of selected system functions as part of contingency plan testing.		
IHGIN Response	Backups are fully tested as part of the IT disaster recovery plan and security policy.		

Control ID	**CP-9(3)**	Control Name	**SEPARATE STORAGE FOR CRITICAL INFORMATION**
Definition	Store backup copies of [Assignment: organization-defined critical system software and other security-related information] in a separate facility or in a fire-rated container that is not collocated with the operational system.		
IHGIN Response	Back-ups are stored in a geographically redundant configuration to ensure operation needs are met.		

Control ID	**CP-9(4)**	Control Name	**PROTECTION FROM UNAUTHORIZED MODIFICATION**
Definition	Deprecated (Implemented in CP-9)		
IHGIN Response	See response to CP-9		

Control ID	**CP-9(5)**	Control Name	**TRANSFER TO ALTERNATE STORAGE SITE**
Definition	Transfer system backup information to the alternate storage site [Assignment: organization-defined time-period and transfer rate consistent with the recovery time and recovery point objectives].		
IHGIN Response	Backup information is maintained within the cloud and onsite to ensure operational needs can be met in the face of a disaster.		

Control ID	**CP-9(6)**	Control Name	**REDUNDANT SECONDARY SYSTEM**
Definition	Conduct system backup by maintaining a redundant secondary system that is not collocated with the primary system and that can be activated without loss of information or disruption to operations		
IHGIN Response	The cloud-based backup has been configured to bring servers on-line in the cloud until a new local system can be configured to be restored to.		

Control ID	**CP-9(7)**	Control Name	**DUAL AUTHORIZATION**
Definition	Enforce dual authorization for the deletion or destruction of [Assignment: organization defined backup information].		
IHGIN Response	Dual authorization for removal of backups has been configured.		

Control ID	**CP-9(8)**	Control Name	**CRYPTOGRAPHIC PROTECTION**
Definition	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of [Assignment: organization-defined backup information].		
IHGIN Response	Systems backups take place on-site and off-site nightly. The on-site backups are encrypted at rest, and the cloud-based backup and recovery is encrypted in transit and at rest. These backups are monitored to ensure they are always operational.		

Control ID	**CP-10**	Control Name	**System Recovery and Reconstitution**
Definition	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time-period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure		
IHGIN Response	The cloud-based backup has been configured to bring servers on-line in the cloud until a new local system can be configured to be restored to.		

Control ID	**CP-10(1)**	Control Name	**CONTINGENCY PLAN TESTING**
Definition	Deprecated (Implemented in CP-4)		
IHGIN Response	See response to CP-4		

Control ID	**CP-10(2)**	Control Name	**TRANSACTION RECOVERY**
Definition	Implement transaction recovery for systems that are transaction-based.		
IHGIN Response	Transaction recovery is implemented for database transactional systems		

Control ID	**CP-10(3)**	Control Name	**COMPENSATING SECURITY CONTROLS**
Definition	Deprecated		
IHGIN Response	This has been addressed through other controls.		

Control ID	**CP-10(4)**	Control Name	**RESTORE WITHIN TIME-PERIOD**
Definition	Provide the capability to restore system components within [Assignment: organization defined restoration time-periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.		
IHGIN Response	IHGIN has the capability to restore systems and services within 24 hours of the disaster event.		

Control ID	**CP-10(5)**	Control Name	**FAILOVER CAPABILITY**
Definition	Deprecated (Implemented in SI-13)		
IHGIN Response	See response to SI-13		

Control ID	**CP-10(6)**	Control Name	**COMPONENT PROTECTION**
Definition	Protect system components used for recovery and reconstitution.		
IHGIN Response	Where needed, specialized hardware components have a redundant component stored off-site for disaster recovery purposes.		

Control ID	**CP-11**	Control Name	**Alternate Communications Protocols**
Definition	Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.		
IHGIN Response	The continued use of current communication protocols will be maintained with backup operations and has been tested as working.		

Control ID	**CP-12**	Control Name	**Safe Mode**
Definition	When [Assignment: organization-defined conditions] are detected, enter a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation]		
IHGIN Response	IHGIN does not support military, civilian space, air traffic, or nuclear power plan operations. Our systems are not configured to have a "safe mode" of operation.		

Control ID	**CP-13**	Control Name	**Alternative Security Mechanisms**
Definition	Employ [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.		
IHGIN Response	Security mechanisms are maintained with restoration of services and backup recovery.		

Control ID	**CP-14**	Control Name	**Self-Challenge**
Definition	Employ [Assignment: organization-defined autonomous service] to [Assignment: organization-defined system or system components] to affect the system or system components in an adverse manner.		
IHGIN Response	The IHGIN disaster recovery plan is tested, and systems are setup and tested using a self-challenge prior to being implemented into the production environment.		

Identification and Authentication

Control ID	**IA-1**	Control Name	**POLICY AND PROCEDURES**

Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] identification and authentication policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and c) Review and update the current identification and authentication: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	Identification and authentication are defined within the IHGIN Security Policy.

Control ID	**IA-2**	Control Name	**Identification and Authentication (Organizational Users)**
Definition	Uniquely identify and authenticate organizational users and associate that unique 5753 identification with processes acting on behalf of those users.		
IHGIN Response	Users are authenticated using active directory or independent application accounts that have been approved by their manager prior to being given access.		

Control ID	**IA-2(1)**	Control Name	**MULTIFACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS**
Definition	Implement multifactor authentication for access to privileged accounts.		
IHGIN Response	Multifactor authentication where available is implemented for IT accounts with privileged access.		

Control ID	**IA-2(2)**	Control Name	**MULTIFACTOR AUTHENTICATION TO NON-PRIVILEGED ACCOUNTS**
Definition	Implement multifactor authentication for access to non-privileged accounts.		
IHGIN Response	Currently non-privileged accounts do not require multifactor authentication. This can be enabled where available if required.		

Control ID	**IA-2(3)**	Control Name	**LOCAL ACCESS TO PRIVILEGED ACCOUNTS**
Definition	Deprecated (Implemented in IA-2(1))		
IHGIN Response	See response to IA-2(1)		

Control ID	**IA-2(4)**	Control Name	**LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS**
Definition	Deprecated (Implemented in IA-2(2))		
IHGIN Response	See response to IA-2(2)		

Control ID	**IA-2(5)**	Control Name	**INDIVIDUAL AUTHENTICATION WITH GROUP AUTHENTICATION**
Definition	When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.		
IHGIN Response	Shared accounts are not used on internal systems. For corporate accounts outside of the organization that are shared across multiple users, they must authenticate to the domain prior to gaining network access.		

Control ID	**IA-2(6)**	Control Name	**ACCESS TO ACCOUNTS — SEPARATE DEVICE**
Definition	Implement multifactor authentication for [Selection (one or more): local; network; remote] access to [Selection (one or more): privileged accounts; non-privileged accounts] such that: a) One of the factors is provided by a device separate from the system gaining access; and b) The device meets [Assignment: organization-defined strength of mechanism requirements].		
IHGIN Response	Where applicable multi-factor authentication uses an authenticator device that has been approved for use by IHGIN IT.		

Control ID	**IA-2(7)**	Control Name	**NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — SEPARATE DEVICE**
Definition	Deprecated (Implemented in IA-2(6))		
IHGIN Response	See response to IA-2(6)		

Control ID	**IA-2(8)**	Control Name	**ACCESS TO ACCOUNTS — REPLAY RESISTANT**
Definition	Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].		
IHGIN Response	IHGIN IT systems use Kerberos authentication where available that protects against replay attacks by exchanging an authenticator during protocol exchanges. Our internal systems use similar methods to ensure that replace attacks are not successful.		

Control ID	**IA-2(9)**	Control Name	**NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS — REPLAY RESISTANT**
Definition	Deprecated (Implemented in IA-2(8))		
IHGIN Response	See response to IA-2(8)		

Control ID	**IA-2(10)**	Control Name	**SINGLE SIGN-ON**
Definition	Provide a single sign-on capability for [Assignment: organization-defined system accounts and services].		
IHGIN Response	SSO is enabled where applicable within the organization. Some applications and systems do not extend this functionality or allow for a federated trust. For those systems, you have to be authenticated to the domain prior to gaining access.		

Control ID	**IA-2(11)**	Control Name	**REMOTE ACCESS — SEPARATE DEVICE**
Definition	Deprecated (Implemented in IA-2(6))		
IHGIN Response	See response to IA-2(6)		

Control ID	**IA-2(12)**	Control Name	**ACCEPTANCE OF PIV CREDENTIALS**
Definition	Accept and electronically verify Personal Identity Verification-compliant credentials.		
IHGIN Response	We currently do not use PIB credentials that are issues by federal agencies for access to our systems.		

Control ID	**IA-2(13)**	Control Name	**OUT-OF-BAND AUTHENTICATION**
Definition	Implement the following out-of-band authentication mechanisms under [Assignment: organization-defined conditions]: [Assignment: organization-defined out-of-band authentication].		
IHGIN Response	We do not use out-of-band authentication currently to authenticate users. This can be implemented if required.		

Control ID	**IA-3**	Control Name	**Device Identification and Authentication**
Definition	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection		
IHGIN Response	Where applicable machines are authenticated by mac address in order to gain network access prior to authenticating the users.		

Control ID	**IA-3(1)**	Control Name	**CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION**
Definition	Authenticate [Assignment: organization-defined devices and/or types of devices] before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.		
IHGIN Response			

Control ID	**IA-3(2)**	Control Name	**CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION**
Definition	Deprecated (Implemented in IA-3(1))		
IHGIN Response	Bidirectional authentication is utilized during key exchange to ensure that clear text passwords are not utilized within IHGIN systems.		

Control ID	**IA-3(3)**	Control Name	**DYNAMIC ADDRESS ALLOCATION**
Definition	a) Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with [Assignment: organization-defined lease information and lease duration]; and b) Audit lease information when assigned to a device.		
IHGIN Response	IHGIN utilized DHCP for device address allocation. Leases are recorded and audited using the IHGIN SIEM solution. New devices are flagged for review.		

Control ID	**IA-3(4)**	Control Name	**DEVICE ATTESTATION**
Definition	Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].		
IHGIN Response	Currently device attestation is not utilized. This can be implemented if required by the client.		

Control ID	**IA-4**	Control Name	**Identifier Management**
Definition	a) Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier; b) Selecting an identifier that identifies an individual, group, role, service, or device; c) Assigning the identifier to the intended individual, group, role, service, or device; and d) Preventing reuse of identifiers for [Assignment: organization-defined time-period].		
IHGIN Response	Mac addresses, ip addresses, and cryptographic certificates are used to ensure that devices, systems, and users cannot reuse credentials or access network and data resources without being uniquely identified.		

Control ID	**IA-4(1)**	Control Name	**PROHIBIT ACCOUNT IDENTIFIERS AS PUBLIC IDENTIFIERS**
Definition	Prohibit the use of system account identifiers that are the same as public identifiers for individual accounts.		
IHGIN Response	System account identifiers are separate from public identifiers.		

Control ID	**IA-4(2)**	Control Name	**SUPERVISOR AUTHORIZATION**
Definition	Deprecated (Implemented in IA-12(1))		
IHGIN Response	See response to IA-12(1)		

Control ID	**IA-4(3)**	Control Name	**MULTIPLE FORMS OF CERTIFICATION**
Definition	Deprecated (Implemented in IA-12(1))		

IHGIN Response	See response to IA-12(2)

Control ID	**IA-4(4)**	Control Name	**IDENTIFY USER STATUS**
Definition	Manage individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].		
IHGIN Response	Each user is uniquely identified by their account name.		

Control ID	**IA-4(5)**	Control Name	**DYNAMIC MANAGEMENT**
Definition	Manage individual identifiers dynamically in accordance with [Assignment: organization defined dynamic identifier policy].		
IHGIN Response	Unique session keys are utilized to dynamically identify the user and session on internal applications. This allows us to create non-repudiation in the case of an internal breach of policy or protocol.		

Control ID	**IA-4(6)**	Control Name	**CROSS-ORGANIZATION MANAGEMENT**
Definition	Coordinate with the following external organizations for cross-organization management of identifiers: [Assignment: organization-defined external organizations].		
IHGIN Response	Currently we do not authenticate across separate organizations. External organizations authenticating to our internal SFTP server and web based applications are provided with authentication credentials that are unique for each user.		

Control ID	**IA-4(7)**	Control Name	**IN-PERSON REGISTRATION**
Definition	Deprecated (Implemented in IA-12(4))		
IHGIN Response	See response to IA-12(4)		

Control ID	**IA-4(8)**	Control Name	**PAIRWISE PSEUDONYMOUS IDENTIFIERS**
Definition	Generate pairwise pseudonymous identifiers.		
IHGIN Response	IHGIN currently does not use pairwise pseudonymous identifiers for ingesting external data sources. We have the capability to implement this if required.		

Control ID	**IA-4(9)**	Control Name	**ATTRIBUTE MAINTENANCE AND PROTECTION**
Definition	Maintain the attributes for each uniquely identified individual, device, or service in [Assignment: organization-defined protected central storage].		
IHGIN Response	User attributes are centrally maintained in each database and audited by our SIEM solution.		

Control ID	**IA-5**	Control Name	**Authenticator Management**
Definition	Manage system authenticators by:		

	a) Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator; b) Establishing initial authenticator content for any authenticators issued by the organization; c) Ensuring that authenticators have sufficient strength of mechanism for their intended use; d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators; e) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; f) Changing default authenticators prior to first use; g) Changing or refreshing authenticators [Assignment: organization-defined time-period by authenticator type]; h) Protecting authenticator content from unauthorized disclosure and modification; i) Requiring individuals to take, and having devices implement, specific controls to protect authenticators; and j) Changing authenticators for group or role accounts when membership to those accounts changes.
IHGIN Response	Default passwords are not allowed to be deployed within the IHGIN network. Systems are to be changed to unique identifiers prior to being implemented. Authenticators are treated similar to passwords and have a lifecycle applied to them along with strength requirements outlined within the IHGIN Security Policy.

Control ID	**IA-5(1)**	Control Name	**PUBLIC KEY-BASED AUTHENTICATION**
Definition	For password-based authentication: a) Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly; b) Verify, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected, or compromised passwords; c) Transmit only cryptographically-protected passwords; d) Store passwords using an approved hash algorithm and salt, preferably using a keyed hash; e) Require immediate selection of a new password upon account recovery; f) Allow user selection of long passwords and passphrases, including spaces and all printable characters; g) Employ automated tools to assist the user in selecting strong password authenticators; and h) Enforce the following composition and complexity rules: [Assignment: organization6091 defined composition and complexity rules].		

IHGIN Response	The IHGIN password policy is outlined in the IHGIN Security Policy.

Control ID	**IA-5(2)**	Control Name	**IN-PERSON OR TRUSTED EXTERNAL PARTY REGISTRATION**
Definition	a) For public key-based authentication 1. Enforce authorized access to the corresponding private key; and 2. Map the authenticated identity to the account of the individual or group; and b) When public key infrastructure (PKI) is used: 1. Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and 2. Implement a local cache of revocation data to support path discovery and validation.		
IHGIN Response	PKI is utilized on the SFTP server. We utilized a signed certificate on our website using a root trust authority.		

Control ID	**IA-5(3)**	Control Name	**AUTOMATED SUPPORT FOR PASSWORD STRENGTH DETERMINATION**
Definition	Deprecated (Implemented in IA-12(4))		
IHGIN Response	See response to IA-12(4)		

Control ID	**IA-5(4)**	Control Name	**CHANGE AUTHENTICATORS PRIOR TO DELIVERY**
Definition	Deprecated (Implemented in IA-5(1))		
IHGIN Response	See response to IA-5(1)		

Control ID	**IA-5(5)**	Control Name	**PROTECTION OF AUTHENTICATORS**
Definition	Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.		
IHGIN Response	IHGIN requires authenticators to be changed from their default values prior to implementation into the production environment.		

Control ID	**IA-5(6)**	Control Name	**POLICY AND PROCEDURES**
Definition	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.		
IHGIN Response	Authenticators are utilized with privileged accounts and only provide access to the information required. Different authenticators are utilized for different systems levels.		

Control ID	**IA-5(7)**	Control Name	**NO EMBEDDED UNENCRYPTED STATIC AUTHENTICATORS**
Definition	Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage		

IHGIN Response	Unencrypted authenticators are prohibited from use.

Control ID	**IA-5(8)**	Control Name	**MULTIPLE SYSTEM ACCOUNTS**
Definition	Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.		
IHGIN Response	Separate authenticators are used for certain systems to ensure that privileged accounts being used across multiple systems have to authenticate using 2-factors.		

Control ID	**IA-5(9)**	Control Name	**FEDERATED CREDENTIAL MANAGEMENT**
Definition	Use the following external organizations to federate authenticators: [Assignment: organization-defined external organizations].		
IHGIN Response	IHGIN uses federated services where supported.		

Control ID	**IA-5(10)**	Control Name	**DYNAMIC CREDENTIAL BINDING**
Definition	Bind identities and authenticators dynamically using the following rules: [Assignment: organization-defined binding rules].		
IHGIN Response	We do not allow credentials to be dynamically allocated based upon a 2nd factor. Credentials are assigned by IT to each user manually and confirmed to meet the principle of least access/privilege.		

Control ID	**IA-5(11)**	Control Name	**HARDWARE TOKEN-BASED AUTHENTICATION**
Definition	Deprecated (Implemented in IA-2(1) & IA-2(2))		
IHGIN Response	See response to IA-2(1) & IA-2(2)		

Control ID	**IA-5(12)**	Control Name	**BIOMETRIC AUTHENTICATION PERFORMANCE**
Definition	For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements [Assignment: organization-defined biometric quality requirements].		
IHGIN Response	IHGIN currently does not utilized biometric controls within the organization. This can be implemented if required.		

Control ID	**IA-5(13)**	Control Name	**EXPIRATION OF CACHED AUTHENTICATORS**
Definition	Prohibit the use of cached authenticators after [Assignment: organization-defined time period].		
IHGIN Response	If cached authenticator information is out of date it is not longer accepted.		

Control ID	**IA-5(14)**	Control Name	**MANAGING CONTENT OF PKI TRUST STORES**
Definition	For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications.		
IHGIN Response	IHGIN utilizes a root authority signed wildcard ssl certification to manage content through the organization.		

Control ID	**IA-5(15)**	Control Name	**GSA-APPROVED PRODUCTS AND SERVICES**
Definition	Use only General Services Administration-approved and validated products and services for identity, credential, and access management.		
IHGIN Response	Currently IHGIN does not have this requirement, but ensures that customer facing systems and systems containing PII are GSA approved where applicable.		

Control ID	**IA-5(16)**	Control Name	**IN-PERSON OR TRUSTED EXTERNAL PARTY AUTHENTICATOR ISSUANCE**
Definition	Require that the issuance of [Assignment: organization-defined types of and/or specific authenticators] be conducted [Selection: in person; by a trusted external party] before [Assignment: organization-defined registration authority] with authorization by [Assignment: organization-defined personnel or roles].		
IHGIN Response	Authenticators are issued by IT in person.		

Control ID	**IA-5(17)**	Control Name	**PRESENTATION ATTACK DETECTION FOR BIOMETRIC AUTHENTICATORS**
Definition	Employ presentation attack detection mechanisms for biometric-based authentication.		
IHGIN Response	IHGIN does not currently use biometric-based authentication on enterprise devices or systems. If implemented, controls will be implemented to ensure that presentation attacks are mitigated.		

Control ID	**IA-5(18)**	Control Name	**PASSWORD MANAGERS**
Definition	a) Employ [Assignment: organization-defined password managers] to generate and manage passwords; and b) Protect the passwords using [Assignment: organization-defined controls].		
IHGIN Response	IHGIN utilized LAPS as an enterprise password management solution for local administrative users. Password repositories and managers are not utilized by staff at this time due to security concerns internally.		

Control ID	**IA-6**	Control Name	**Authenticator Feedback**
Definition	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.		
IHGIN Response	Authenticators in use meet all compliance standards and feedback from systems is limited to prevent attacks.		

Control ID	**IA-7**	Control Name	**Cryptographic Module Authentication**
Definition	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.		
IHGIN Response	Cryptographic standards used currently meet all applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for authentication.		

Control ID	**IA-8**	Control Name	**Identification and Authentication (Non-Organizational Users)**
Definition	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.		
IHGIN Response	IHGIN currently does not access federal information or systems that are sensitive. Non-organizational users are required to authenticate over an encrypted connection.		

Control ID	**IA-8(1)**	Control Name	**ACCEPTANCE OF PIV CREDENTIALS FROM OTHER AGENCIES**
Definition	Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.		
IHGIN Response	IHGIN does not currently use PIV credentials provided by federal agencies.		

Control ID	**IA-8(2)**	Control Name	**ACCEPTANCE OF EXTERNAL PARTY CREDENTIALS**
Definition	Accept only external credentials that are NIST-compliant.		
IHGIN Response	IHGIN allows each customer to provide a level of credentials that are comfortable for their users. We take precautions to ensure that auditing and alterting is done on accounts to prevent breaches internally. We prefer customers to use NIST SP 800-63-3 IAL2|AAL2|FAL2 level compliance. In cases where not possible, connections and authentication into the environment must comply with the IHGIN IT Security Policy that outlines password and cryptographic requirements.		

Control ID	**IA-8(3)**	Control Name	**USE OF FICAM-APPROVED PRODUCTS**
Definition	Deprecated (Implemented in IA-8(2))		
IHGIN Response	See response to IA-8(2)		

Control ID	**IA-8(4)**	Control Name	**USE OF NIST-ISSUED PROFILES**
Definition	Conform to NIST-issued profiles for identity management		
IHGIN Response	IHGIN allows each customer to provide a level of credentials that are comfortable for their users. We take precautions to ensure that auditing and alterting is done on accounts to prevent breaches internally. We prefer customers to use NIST SP 800-63-3 IAL2|AAL2|FAL2 level compliance. In cases where not possible, connections and authentication into the environment must comply with the IHGIN IT Security Policy that outlines password and cryptographic requirements.		

Control ID	**IA-8(5)**	Control Name	**ACCEPTANCE OF PIV-I CREDENTIALS**
Definition	Accept and verify federated or PKI credentials that meet [Assignment: organization defined policy].		
IHGIN Response	IHGIN does not currently use PIV credentials provided by federal agencies.		

Control ID	**IA-8(6)**	Control Name	**DISASSOCIABILITY**
Definition	Implement the following measures to disassociate user attributes or credential assertion relationships among individuals, credential service providers, and relying parties: [Assignment: organization-defined measures].		
IHGIN Response	Encryption is utilized to blond credential service providers and relying parties from each other in order to make identity attributes less visible where possible when utilizing federated services.		

Control ID	**IA-9**	Control Name	**Service Identification and Authentication**
Definition	Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.		
IHGIN Response	Unique identification is required before communications is established with devices users, or other applications/services. Kerberos is one example of how this is accomplished within the IHGIN production environment.		

Control ID	**IA-9(1)**	Control Name	**INFORMATION EXCHANGE**
Definition	Deprecated (Implemented in IA-9)		
IHGIN Response	See response to IA-9		

Control ID	**IA-9(2)**	Control Name	**TRANSMISSION OF DECISIONS**
Definition	Deprecated (Implemented in IA-9)		
IHGIN Response	See response to IA-9		

Control ID	**IA-10**	Control Name	**Adaptive Authentication**
Definition	Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].		
IHGIN Response	Systems are audited in real-time by our SIEM solution. Any account authenticated the appears to be conducting suspicious behavior is disabled and IT alerts to investigate.		

Control ID	**IA-11**	Control Name	**Re-authentication**
Definition	Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].		

IHGIN Response	Re-authentication is required within the IHGIN IT Security Policy.

Control ID	**IA-12**	Control Name	**Identity Proofing**
Definition	a) Identity proof users that require accounts for logical access to systems based on appropriate identity assurance level requirements as specified in applicable standards and guidelines; b) Resolve user identities to a unique individual; and c) Collect, validate, and verify identity evidence		
IHGIN Response	IHGIN does not allow registration of accounts, they are assigned by IT after a need for access has been established.		

Control ID	**IA-12(1)**	Control Name	**SUPERVISOR AUTHORIZATION**
Definition	Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.		
IHGIN Response	IHGIN does not allow registration of accounts, they are assigned by IT after a need for access has been established. This required supervisor authorization.		

Control ID	**IA-12(2)**	Control Name	**IDENTITY EVIDENCE**
Definition	Require evidence of individual identification be presented to the registration authority		
IHGIN Response	IHGIN requires individual managerial approval to provide access to a system. For customer facing systems, IHGIN relies on the customer to ensure that accounts created are given only to those in need of access.		

Control ID	**IA-12(3)**	Control Name	**IDENTITY EVIDENCE VALIDATION AND VERIFICATION**
Definition	Require that the presented identity evidence be validated and verified through [Assignment: organizational defined methods of validation and verification].		
IHGIN Response	Internally IHGIN ensures that identity validation and verification is taking place. Externally, IHGIN relies on customers to manage their accounts and access internally.		

Control ID	**IA-12(4)**	Control Name	**IN-PERSON VALIDATION AND VERIFICATION**
Definition	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority		
IHGIN Response	Where applicable IHGIN requires validation of identity in person prior to providing credentials.		

Control ID	**IA-12(5)**	Control Name	**ADDRESS CONFIRMATION**
Definition	Require that a [Selection: registration code; notice of proofing] be delivered through an out-of-band channel to verify the users address (physical or digital) of record.		
IHGIN Response	At this time, this is not required. It can be implemented if required by the customer.		

Control ID	**IA-12(6)**	Control Name	**ACCEPT EXTERNALLY-PROOFED IDENTITIES**
Definition	Accept externally-proofed identities at [Assignment: organization-defined identity assurance level].		
IHGIN Response	IHGIN internally does not accept externally proofed identities. For customer systems, IHGIN will accept that the customer has externally proofed the identity prior to issuing credentials.		

Incident Response

Control ID	**IR-1**	Control Name	**POLICY AND PROCEDURES**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] incident response policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the incident response policy and the associated incident response controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and c) Review and update the current incident response: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN has highlighted incident response requirements within the Disaster Recovery Plan. Incident response is designed to exceed the needs of the customer. The sections of this control as applicable are being met be IHGIN.		

Control ID	**IR-2**	Control Name	**Incident Response Training**
Definition	Provide incident response training to system users consistent with assigned roles and responsibilities: a) Within [Assignment: organization-defined time-period] of assuming an incident response role or responsibility or acquiring system access; b) When required by system changes; and c) [Assignment: organization-defined frequency] thereafter		
IHGIN Response	IHGIN utilizes simulated and paper-based events/exercises as a form of incident response training. This is done to ensure that users understand their role in incident response and that IHGIN can adapt the Disaster Recovery Plan in order to best facilitate response.		

Control ID	**IR-2(1)**	Control Name	**SIMULATED EVENTS**

Definition	Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.
IHGIN Response	IHGIN utilizes simulated and paper-based events/exercises as a form of incident response training. This is done to ensure that users understand their role in incident response and that IHGIN can adapt the Disaster Recovery Plan in order to best facilitate response.

Control ID	**IR-2(2)**	Control Name	**AUTOMATED TRAINING ENVIRONMENTS**
Definition	Provide an incident response training environment using [Assignment: organization defined automated mechanisms]		
IHGIN Response	IHGIN encourages IT staff to take part in external training environments and exercises and share their experiences internally.		

Control ID	**IR-3**	Control Name	**Incident Response Testing**
Definition	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].		
IHGIN Response	During incident response testing, IHGIN are required to meet the business requirements that have been outlined internally for restoration of services. In cases where this may not be met during an exercise, changes to the plan are implemented in order to facilitate a better response in the future.		

Control ID	**IR-3(1)**	Control Name	**AUTOMATED TESTING**
Definition	Test the incident response capability using [Assignment: organization-defined automated mechanisms]		
IHGIN Response	IHGIN has automated testing that occurs to test end-user response to potential security events.		

Control ID	**IR-3(2)**	Control Name	**COORDINATION WITH RELATED PLANS**
Definition	Coordinate incident response testing with organizational elements responsible for related plans.		
IHGIN Response	The Disaster Recovery Plan and Incident Response Plan are coordinated with other internal documented plans to ensure operation cohesion in the case of a disaster event.		

Control ID	**IR-3(3)**	Control Name	**CONTINUOUS IMPROVEMENT**
Definition	Use qualitative and quantitative data from testing to: a) Determine the effectiveness of incident response processes; b) Continuously improve incident response processes; and c) Provide incident response measures and metrics that are accurate, consistent, and in a reproducible format.		
IHGIN Response	IHGIN tests the incident response plan and reviews it regularly to look for areas to improve response.		

Control ID	**IR-4**	Control Name	**Incident Handling**
Definition	a) Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery; b) Coordinate incident handling activities with contingency planning activities; c) Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and d) Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.		
IHGIN Response	Incident handling procedures are outlined in the disaster recovery plan. Incident handling follows the procedure of identification, data collection, isolation, response, recovery, additional investigation and reporting.		

Control ID	**IR-4(1)**	Control Name	**AUTOMATED INCIDENT HANDLING PROCESSES**
Definition	Support the incident handling process using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	Automated collection of logs and information is conducted as part of the incident handling procedure to expedite the process into the isolation phase.		

Control ID	**IR-4(2)**	Control Name	**DYNAMIC RECONFIGURATION**
Definition	Include the following types of dynamic reconfiguration for [Assignment: organization defined system components] as part of the incident response capability: [Assignment: organization-defined types of dynamic reconfiguration].		
IHGIN Response	The firewall system and SIEM solutions both allow for some dynamic configuration of items to occur during incident handling. For example, detected intrusion attempts will blacklist an IP address, or multiple login attempts with an admin account will trigger notification of IT staff.		

Control ID	**IR-4(3)**	Control Name	**CONTINUITY OF OPERATIONS**
Definition	Identify [Assignment: organization-defined classes of incidents] and take the following actions in response to those incidents to ensure continuation of organizational missions and business functions: [Assignment: organization-defined actions to take in response to classes of incidents].		
IHGIN Response	IT has a full disaster recovery plan that allows for the continuity of operations.		

Control ID	**IR-4(4)**	Control Name	**INFORMATION CORRELATION**
Definition	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.		
IHGIN Response	The SIEM solution and log collector service allows for information to be correlated across multiple systems and services.		

Control ID	**IR-4(5)**	Control Name	**AUTOMATIC DISABLING OF SYSTEM**
Definition	Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected.		
IHGIN Response	In some cases, access to a system will be disabled by the firewall in a fail safe configuration in the case of a detected attack against a system.		

Control ID	**IR-4(6)**	Control Name	**INSIDER THREATS — SPECIFIC CAPABILITIES**
Definition	Implement an incident handling capability for incidents involving insider threats.		
IHGIN Response	Internally users are assigned a baseline of normal usage within the environment by our SIEM solution. Any attempts to access data or user behavior considered to be abnormal is flagged for review by IT.		

Control ID	**IR-4(7)**	Control Name	**INSIDER THREATS — INTRA-ORGANIZATION COORDINATION**
Definition	Coordinate an incident handling capability for insider threats that includes the following organizational entities [Assignment: organization-defined entities].		
IHGIN Response	Internally users are assigned a baseline of normal usage within the environment by our SIEM solution. Any attempts to access data or user behavior considered to be abnormal is flagged for review by IT. This applies as well to intra-organizational threats.		

Control ID	**IR-4(8)**	Control Name	**CORRELATION WITH EXTERNAL ORGANIZATIONS**
Definition	Coordinate with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross organization perspective on incident awareness and more effective incident responses.		
IHGIN Response	IHGIN coordinates with other companies under the WIHG umbrella of companies and other organizations within the Toennjes empire to identify potential organizational and cyber risk.		

Control ID	**IR-4(9)**	Control Name	**DYNAMIC RESPONSE CAPABILIT**
Definition	Employ [Assignment: organization-defined dynamic response capabilities] to respond to incidents.		
IHGIN Response	IHGIN has the capability to deploy new or replacement organizational capabilities in response to incidents. This includes capabilities implemented at the mission and business process level and at the system level.		

Control ID	**IR-4(10)**	Control Name	**SUPPLY CHAIN COORDINATION**
Definition	Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain		
IHGIN Response	IHGIN has coordinated efforts with supply chain vendors to ensure that the handoff of materials and information is done in a secure manner and an alternate form of handoff is in place in the case that an cyber event were to take place.		

Control ID	**IR-4(11)**	Control Name	**INTEGRATED INCIDENT RESPONSE TEAM**

Definition	Establish and maintain an integrated incident response team that can be deployed to any location identified by the organization in [Assignment: organization-defined time period].
IHGIN Response	The IHGIN incident response team can be deployed to any IHG location.

Control ID	**IR-4(12)**	Control Name	**MALICIOUS CODE AND FORENSIC ANALYSIS**
Definition	Analyze [Selection (one or more): malicious code; [Assignment: organization-defined residual artifacts] remaining in the system after the incident.		
IHGIN Response	If an incident involving malicious code enter the environment was to take place, it is submitted to the IHGIN security vendor for forensic analysis. Internal forensic analysis takes place to create any additional levels of security required.		

Control ID	**IR-4(13)**	Control Name	**BEHAVIOR ANALYSIS**
Definition	Analyze anomalous or suspected adversarial behavior in or related to [Assignment: organization-defined environments or resources].		
IHGIN Response	The IHGIN internal SIEM solution provides anomalous behavior detection.		

Control ID	**IR-4(14)**	Control Name	**SECURITY OPERATIONS CENTER**
Definition	Establish and maintain a security operations center.		
IHGIN Response	IHGIN does not maintain an active SOC but does utilize soc SIEM systems and response techniques to monitor for security events at their Amherst facility. If required, a fully operational SOC can be established.		

Control ID	**IR-4(15)**	Control Name	**PUBLIC RELATIONS AND REPUTATION REPAIR**
Definition	a) Manage public relations associated with an incident; and b) Employ measures to repair the reputation of the organization.		
IHGIN Response	IHGIN deploys an account manager to actively manage and IT security events and provide direct to customer interaction before, during, and after any security events.		

Control ID	**IR-5**	Control Name	**Incident Monitoring**
Definition	Track and document security, privacy, and supply chain incidents.		
IHGIN Response	IHGIN monitors for incidents and investigates and documents events as they occur.		

Control ID	**IR-5(1)**	Control Name	**AUTOMATED TRACKING, DATA COLLECTION, AND ANALYSIS**
Definition	Track security and privacy incidents and collect and analyze incident information using [Assignment: organization-defined automated mechanisms]		
IHGIN Response	IHGIN automatically collects data in relation to security incidents using the internal SIEM solution.		

Control ID	**IR-6**	Control Name	**Incident Reporting**
Definition	a) Require personnel to report suspected security, privacy, and supply chain incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and b) Report security, privacy, and supply chain incident information to [Assignment: organization defined authorities].		
IHGIN Response	IHGIN reports any security breaches as required contractually and by law. Any incidents that may impact clients are reported to clients immediately upon discovery and they are responded to appropriately.		

Control ID	**IR-6(1)**	Control Name	**AUTOMATED REPORTING**
Definition	Report incidents using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	IHGIN does not provide automated reports of possible security incidents to clients. These are investigated and verified prior to disclosure internally as to not alarm anyone with false positives.		

Control ID	**IR-6(2)**	Control Name	**VULNERABILITIES RELATED TO INCIDENTS**
Definition	Report system vulnerabilities associated with reported incidents to [Assignment: organization-defined personnel or roles].		
IHGIN Response	IHGIN uses a vulnerability assessment solution to scan systems and report on any potential vulnerabilities that may exist.		

Control ID	**IR-6(3)**	Control Name	**SUPPLY CHAIN COORDINATION**
Definition	Provide security and privacy incident information to the provider of the product or service and other organizations involved in the supply chain for systems or system components related to the incident.		
IHGIN Response	IHGIN provides security incident information to supply chain partners for any systems or systems components they have on-site in relation to the incident.		

Control ID	**IR-7**	Control Name	**Incident Response Assistance**
Definition	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of security, privacy, and supply chain incidents.		
IHGIN Response	IHGIN can contract incident response externally under certain circumstances that may make it difficult to handle internally.		

Control ID	**IR-7(1)**	Control Name	**AUTOMATION SUPPORT FOR AVAILABILITY OF INFORMATION AND SUPPORT**
Definition	Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	IHGIN does not have external assistance and support automated at this time. This can be done if required by the customer.		

Control ID	**IR-7(2)**	Control Name	**COORDINATION WITH EXTERNAL PROVIDERS**
Definition	a) Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and b) Identify organizational incident response team members to the external providers.		
IHGIN Response	IHGIN tries to be as cooperative in the coordination of security operations with external partners and providers as possible. The level of cooperation and coordination depends on an internal risk assessment to ensure that the organization isn't taking on any undue risk.		

Control ID	**IR-8**	Control Name	**Incident Response Plan**
Definition	a) Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability; 3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; 8. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and 9. Explicitly designates responsibility for incident response to [Assignment: organization defined entities, personnel, or roles]. b) Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; c) Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing; d) Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and e) Protect the incident response plan from unauthorized disclosure and modification		
IHGIN Response	IHGIN covers this information under the Disaster Recovery and Incident Response Plan.		

Control ID	**IR-8(1)**	Control Name	**PRIVACY BREACHES**
Definition	Include the following in the Incident Response Plan for breaches involving personally identifiable information:		

	a) A process to determine if notice to individuals or other organizations, including oversight organizations, is needed; b) An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and c) Identification of applicable privacy requirements.
IHGIN Response	IHGIN follows the reporting requirements outlined by Indiana's Security Breach Notification Statute (Indiana Code Article 24-4.9).

Control ID	**IR-9**	Control Name	**Information Spillage Response**
Definition	Respond to information spills by: a) Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills; b) Identifying the specific information involved in the system contamination; c) Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill; d) Isolating the contaminated system or system component; e) Eradicating the information from the contaminated system or component; f) Identifying other systems or system components that may have been subsequently contaminated; and g) Performing the following additional actions: [Assignment: organization-defined actions].		
IHGIN Response	IHGIN avoids information spillage through auditing data and data access throughout the organization. If data is discovered to have moved from a protected system it is blocked and flagged for review by IT staff.		

Control ID	**IR-9(1)**	Control Name	**RESPONSIBLE PERSONNEL**
Definition	Deprecated (Implemented in IR-9)		
IHGIN Response	See response to IR-9		

Control ID	**IR-9(2)**	Control Name	**TRAINING**
Definition	Provide information spillage response training [Assignment: organization-defined frequency].		
IHGIN Response	Information spillage and avoidance is part of the ongoing cyber security training iniative undertaken by IHGIN.		

Control ID	**IR-9(3)**	Control Name	**POST-SPILL OPERATIONS**
Definition	Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: [Assignment: organization-defined procedures].		

IHGIN Response	In the case that spillage was to take place containment and post-still operations will treat the event similar to a typical incident response.

Control ID	**IR-9(4)**	Control Name	**EXPOSURE TO UNAUTHORIZED PERSONNEL**
Definition	Employ the following controls for personnel exposed to information not within assigned access authorizations: [Assignment: organization-defined controls].		
IHGIN Response	Role based access controls ensure that data is not exposed to unauthorized personnel.		

Control ID	**IR-10**	Control Name	**INTEGRATED INFORMATION SECURITY ANALYSIS**
Definition	Deprecated (Implemented in IR-4(11))		
IHGIN Response	See response to IR-4(11)		

Maintenance

Control ID	**MA-1**	Control Name	**POLICY AND PROCEDURES**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] maintenance policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and c) Review and update the current maintenance: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN has strict maintenance controls including records and schedule for patches, systems maintenance, repair, etc. These systems and policies fall under IHGIN IT Operations and the IHGIN Security Policy.		

Control ID	**MA-2**	Control Name	**Controlled Maintenance**
Definition	a) Schedule, document, and review records of maintenance, repair, or replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;		

	b) Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location; c) Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement; d) Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information]; e) Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and f) Include the following information in organizational maintenance records: [Assignment: organization-defined information].
IHGIN Response	IHGIN ensures that all maintenance follows strict procedures and is documented and audited to ensure that maintenance does not introduce any new security issues into production. In the case of emergency maintenance to systems to patch newly discovered security issues, occasionally full testing of the new patch or system might be skipped as the result of a risk assessment to systems and information. All potentially impacted systems and controls are verified after maintenance to ensure that systems remain in an optimal state.

Control ID	**MA-2(1)**	Control Name	**RECORD CONTENT**
Definition	Deprecated (Implemented in MA-2)		
IHGIN Response	See response to MA-2		

Control ID	**MA-2(2)**	Control Name	**AUTOMATED MAINTENANCE ACTIVITIES**
Definition	a) Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms]; and b) Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.		
IHGIN Response	IHGIN maintains schedules and logs of all maintenance conducted during normal maintenance windows. All emergency maintenance windows are logged.		

Control ID	**MA-3**	Control Name	**Maintenance Tools**
Definition	a) Approve, control, and monitor the use of system maintenance tools; and b) Review previously approved system maintenance tools [Assignment: organization-defined frequency].		
IHGIN Response	Only IHGIN IT staff have access to utilize internal system maintenance tools.		

Control ID	**MA-3(1)**	Control Name	**INSPECT TOOLS**

Definition	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.
IHGIN Response	Where available, changes to systems during maintenance are audited and logged by our SIEM solution and inspected to ensure that new security issues or malware are not introduced into the environment as part of the maintenance process.

Control ID	**MA-3(2)**	Control Name	**INSPECT MEDIA**
Definition	Check media containing diagnostic and test programs for malicious code before the media are used in the system.		
IHGIN Response	IHGIN checks and verifies all media connected to IHGIN systems for malicious code or malformed data prior to use.		

Control ID	**MA-3(3)**	Control Name	**PREVENT UNAUTHORIZED REMOVAL**
Definition	Prevent the removal of maintenance equipment containing organizational information by: a) Verifying that there is no organizational information contained on the equipment; b) Sanitizing or destroying the equipment; c) Retaining the equipment within the facility; or d) Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.		
IHGIN Response	The removal of maintenance equipment and software is done by IHGIN IT staff and the destruction of any data is done at the software and physical layer at end of life to ensure no customer data can be recovered.		

Control ID	**MA-3(4)**	Control Name	**RESTRICTED TOOL USE**
Definition	Restrict the use of maintenance tools to authorized personnel only		
IHGIN Response	IHGIN restricts the use of maintenance tools to IT staff only.		

Control ID	**MA-3(5)**	Control Name	**EXECUTION WITH PRIVILEGE**
Definition	Monitor the use of maintenance tools that execute with increased privilege		
IHGIN Response	Any use of programs by privileged users is recorded and audited by our SIEM solution.		

Control ID	**MA-3(6)**	Control Name	**SOFTWARE UPDATES AND PATCHES**
Definition	Inspect maintenance tools to ensure the latest software updates and patches are installed.		
IHGIN Response	IHGIN monitors software, systems, and exploit databases to ensure that all security patches and updates are applied to systems within the organization.		

Control ID	**MA-4**	Control Name	**Nonlocal Maintenance**
Definition	a) Approve and monitor nonlocal maintenance and diagnostic activities;		

	b) Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system; c) Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions; d) Maintain records for nonlocal maintenance and diagnostic activities; and e) Terminate session and network connections when nonlocal maintenance is completed.
IHGIN Response	If nonlocal maintenance is required by a vendor, the access to the machine is controlled and visually monitored by IT staff. Any changes to configurations have to be vetted by IT prior to implementation.

Control ID	**MA-4(1)**	Control Name	**LOGGING AND REVIEW**
Definition	a) Log [Assignment: organization-defined audit events] for nonlocal maintenance and diagnostic sessions; and b) Review the audit records of the maintenance and diagnostic sessions		
IHGIN Response	IHGIN SIEM solution reviews all audit records and logs in real-time.		

Control ID	**MA-4(2)**	Control Name	**DOCUMENT NONLOCAL MAINTENANCE**
Definition	Deprecated (Implemented in MA-1 & MA-4)		
IHGIN Response	See response to MA-1 & MA-4		

Control ID	**MA-4(3)**	Control Name	**COMPARABLE SECURITY AND SANITIZATION**
Definition	a) Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or b) Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.		
IHGIN Response	IHGIN will only vendors with comparable security controls in place to access systems to conduct maintenance actions under the supervision of IHGIN IT staff.		

Control ID	**MA-4(4)**	Control Name	**AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS**
Definition	Protect nonlocal maintenance sessions by: a) Employing [Assignment: organization-defined authenticators that are replay resistant]; and b) Separating the maintenance sessions from other network sessions with the system by either: 1. Physically separated communications paths; or 2. Logically separated communications paths		

IHGIN Response	Communications paths are logically separated using encryption.

Control ID	**MA-4(5)**	Control Name	**APPROVALS AND NOTIFICATIONS**
Definition	a) Require the approval of each nonlocal maintenance session by [Assignment: organization-defined personnel or roles]; and b) Notify the following personnel or roles of the date and time of planned nonlocal maintenance: [Assignment: organization-defined personnel or roles].		
IHGIN Response	Each non-local maintenance session has to be approved by the Enterprise Architect and has to be monitored and supervised by IT staff.		

Control ID	**MA-4(6)**	Control Name	**CRYPTOGRAPHIC PROTECTION**
Definition	Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: [Assignment: organization-defined cryptographic mechanisms].		
IHGIN Response	Nonlocal maintenance must use a secure cryptographic channel using only approved software for access.		

Control ID	**MA-4(7)**	Control Name	**DISCONNECT VERIFICATION**
Definition	Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.		
IHGIN Response	Nonlocal maintenance connections must be verified as closed by IT prior to finalizing any tickets related to the maintenance.		

Control ID	**MA-5**	Control Name	**Maintenance Personnel**
Definition	a) Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel; b) Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and c) Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.		
IHGIN Response	Only IT staff are authorized to conduct maintenance. Any external contractor conducting IT maintenance is escorted by IHGIN IT staff while on-site at all times.		

Control ID	**MA-5(1)**	Control Name	**INDIVIDUALS WITHOUT APPROPRIATE ACCESS**
Definition	a) Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: 1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the		

	system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; 2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and b) Develop and implement [Assignment: organization-defined alternate controls] in the event a system component cannot be sanitized, removed, or disconnected from the system
IHGIN Response	IHGIN does not handle secret or top-secret data at any level.

Control ID	**MA-5(2)**	Control Name	**SECURITY CLEARANCES FOR CLASSIFIED SYSTEM**
Definition	Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for compartments of information on the system.		
IHGIN Response	IHGIN does not handle secret or top-secret data at any level. IHGIN does require IT security professional to have a valid citizenship from a five eyes nation.		

Control ID	**MA-5(3)**	Control Name	**CITIZENSHIP REQUIREMENTS FOR CLASSIFIED SYSTEMS**
Definition	Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are U.S. citizens.		
IHGIN Response	IHGIN does not handle secret or top-secret data at any level.		

Control ID	**MA-5(4)**	Control Name	**FOREIGN NATIONALS**
Definition	Verify that: a) Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within Memoranda of Agreements.		
IHGIN Response	IHGIN does not handle secret or top-secret data at any level.		

Control ID	**MA-5(5)**	Control Name	**NON-SYSTEM MAINTENANCE**
Definition	Verify that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.		

IHGIN Response	IHGIN has strict access controls for contractors while on-site that require them to have appropriate authorization for access into areas that physically house data.

Control ID	**MA-6**	Control Name	**Timely Maintenance**
Definition	Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time-period] of failure		
IHGIN Response	IHGIN has agreements in place with external vendors to ensure that systems can remain operational in the case of physical failure until a replacement can be sourced.		

Control ID	**MA-6(1)**	Control Name	**PREVENTIVE MAINTENANCE**
Definition	Perform preventive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].		
IHGIN Response	IT is alerted to systems issues such as drive space, CPU usage, memory usage in order to take proactive measures and solve issues before they become user facing.		

Control ID	**MA-6(2)**	Control Name	**PREDICTIVE MAINTENANCE**
Definition	Perform predictive maintenance on [Assignment: organization-defined system components] at [Assignment: organization-defined time intervals].		
IHGIN Response	IHGIN performs systems analysis to project timelines for some systems based issues and takes appropriate steps to do maintenance or replace systems prior to end of life or before performance constraints are projected to be met.		

Control ID	**MA-6(3)**	Control Name	**AUTOMATED SUPPORT FOR PREDICTIVE MAINTENANCE**
Definition	Transfer predictive maintenance data to a maintenance management system using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	Certain systems within the organization will automatically conduct predictive maintenance. For example, computer systems will automatically clear our temporary files if drive space reached 90%.		

Control ID	**MA-7**	Control Name	**Field Maintenance**
Definition	Restrict or prohibit field maintenance on [Assignment: organization-defined systems or system components] to [Assignment: organization-defined trusted maintenance facilities].		
IHGIN Response	IHGIN allows IT to conduct field service when on-site.		

Media Protection

Control ID	**MP-1**	Control Name	**POLICY AND PROCEDURES**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:		

	1. [Selection (one or more): organization-level; mission/business process-level; system level] media protection policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and c) Review and update the current media protection: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	IHGIN outlines the procedures and policies around media protection in the IHGIN Security Policy.

Control ID	**MP-2**	Control Name	**Media Access**
Definition	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].		
IHGIN Response	IHGIN restricts access to removable media sources.		

Control ID	**MP-2(1)**	Control Name	**AUTOMATED RESTRICTED ACCESS**
Definition	Deprecated (Implemented in MP-4(2))		
IHGIN Response	See response to MP-4(2)		

Control ID	**MP-2(2)**	Control Name	**CRYPTOGRAPHIC PROTECTION**
Definition	Deprecated (Implemented in SC-28(1))		
IHGIN Response	See response to SC-28(1)		

Control ID	**MP-3**	Control Name	**Media Marking**
Definition	a) Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and b) Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas].		
IHGIN Response	IHGIN does on occasion require the creation of external media for public consumption. This media is labelled and handling is controlled by IHGIN customer service.		

Control ID	**MP-4**	Control Name	**Media Storage**
Definition	a) Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and b) Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.		
IHGIN Response	Physical access to media storage is protected and monitored by magnetic lock and badge access. IHGIN has strict data destruction requirements.		

Control ID	**MP-4(1)**	Control Name	**CRYPTOGRAPHIC PROTECTION**
Definition	Deprecated (Implemented in SC-28(1))		
IHGIN Response	See response to SC-28(1)		

Control ID	**MP-4(2)**	Control Name	**AUTOMATED RESTRICTED ACCESS**
Definition	Restrict access to media storage areas, log access attempts, and access granted using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	Physical access to media storage is protected and monitored by magnetic lock and badge access. This is logged and video monitored.		

Control ID	**MP-5**	Control Name	**Media Transport**
Definition	a) Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls]; b) Maintain accountability for system media during transport outside of controlled areas; c) Document activities associated with the transport of system media; and d) Restrict the activities associated with the transport of system media to authorized personnel.		
IHGIN Response	When sending public information to clients via external media it is sent via registered mail where applicable.		

Control ID	**MP-5(1)**	Control Name	**PROTECTION OUTSIDE OF CONTROLLED AREAS**
Definition	Deprecated (Implemented in MP-5)		
IHGIN Response	See response to MP-5		

Control ID	**MP-5(2)**	Control Name	**DOCUMENTATION OF ACTIVITIES**
Definition	Deprecated (Implemented in MP-5)		
IHGIN Response	See response to MP-5		

Control ID	**MP-5(3)**	Control Name	**CUSTODIANS**

Definition	Employ an identified custodian during transport of system media outside of controlled areas.
IHGIN Response	IHGIN customer service act as a data custodian in the case that public information is being sent externally.

Control ID	**MP-5(4)**	Control Name	**CRYPTOGRAPHIC PROTECTION**
Definition	Deprecated (Implemented in SC-28(1))		
IHGIN Response	See response to SC-28(1)		

Control ID	**MP-6**	Control Name	**Media Sanitization**
Definition	a) Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and b) Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.		
IHGIN Response	IHGIN has extensive media sanitization requirements outlined within the IHGIN Security Policy and Media Disposal Policy.		

Control ID	**MP-6(1)**	Control Name	**REVIEW, APPROVE, TRACK, DOCUMENT, AND VERIFY**
Definition	Review, approve, track, document, and verify media sanitization and disposal actions.		
IHGIN Response	IHGIN has extensive media sanitization requirements outlined within the IHGIN Security Policy and Media Disposal Policy. This includes approving, tracking, documenting, and verifying data destruction and media disposal.		

Control ID	**MP-6(2)**	Control Name	**EQUIPMENT TESTING**
Definition	Test sanitization equipment and procedures [Assignment: organization-defined frequency] to verify that the intended sanitization is being achieved.		
IHGIN Response	All equipment used for data disposal and destruction is tested.		

Control ID	**MP-6(3)**	Control Name	**NONDESTRUCTIVE TECHNIQUES**
Definition	Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].		
IHGIN Response	IHGIN does not allow portable storage devices to be connected to production systems.		

Control ID	**MP-6(4)**	Control Name	**CONTROLLED UNCLASSIFIED INFORMATION**
Definition	Deprecated (Implemented in MP-6)		
IHGIN Response	See response to MP-6		

Control ID	**MP-6(5)**	Control Name	**CLASSIFIED INFORMATION**
Definition	Deprecated (Implemented in MP-6)		
IHGIN Response	See response to MP-6		

Control ID	**MP-6(6)**	Control Name	**MEDIA DESTRUCTION**
Definition	Deprecated (Implemented in MP-6)		
IHGIN Response	See response to MP-6		

Control ID	**MP-6(7)**	Control Name	**DUAL AUTHORIZATION**
Definition	Enforce dual authorization for the sanitization of [Assignment: organization-defined system media].		
IHGIN Response	Destruction of systems and sanitization of data required the approval of IHGIN IT Management and the Manager responsible for the data.		

Control ID	**MP-6(8)**	Control Name	**REMOTE PURGING OR WIPING OF INFORMATION**
Definition	Provide the capability to purge or wipe information from [Assignment: organization defined systems or system components] [Selection: remotely; under the following conditions: [Assignment: organization-defined conditions]].		
IHGIN Response	IHGIN has the capability to purge or remote wipe information from mobile devices.		

Control ID	**MP-7**	Control Name	**Media Use**
Definition	a) Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and b) Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.		
IHGIN Response	External media use is strictly prohibited.		

Control ID	**MP-7(1)**	Control Name	**PROHIBIT USE WITHOUT OWNER**
Definition	Deprecated (Implemented in MP-7)		
IHGIN Response	See response to MP-7		

Control ID	**MP-7(2)**	Control Name	**PROHIBIT USE OF SANITIZATION-RESISTANT MEDIA**
Definition	Prohibit the use of sanitization-resistant media in organizational systems		
IHGIN Response	The use of sanitization resistant media is prohibited within the production environment. In the case that such a system has been utilized within operations, IHGIN IT utilizes the 135 ton hydraulic press to overcome the sanitization resistance.		

Control ID	**MP-8**	Control Name	**Media Downgrading**
Definition	a) Establish [Assignment: organization-defined system media downgrading process] that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information; b) Verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information; c) Identify [Assignment: organization-defined system media requiring downgrading]; and d) Downgrade the identified system media using the established process.		
IHGIN Response	IHGIN does not utilized data classification systems as IHGIN does not have the requirement to store classified information.		

Control ID	**MP-8(1)**	Control Name	**DOCUMENTATION OF PROCESS**
Definition	Document system media downgrading actions.		
IHGIN Response	IHGIN does not utilized data classification systems as IHGIN does not have the requirement to store classified information.		

Control ID	**MP-8(2)**	Control Name	**EQUIPMENT TESTING**
Definition	Test downgrading equipment and procedures [Assignment: organization-defined frequency] to verify that downgrading actions are being achieved.		
IHGIN Response	IHGIN does not utilized data classification systems as IHGIN does not have the requirement to store classified information.		

Control ID	**MP-8(3)**	Control Name	**CONTROLLED UNCLASSIFIED INFORMATION**
Definition	Downgrade system media containing controlled unclassified information prior to public release.		
IHGIN Response	IHGIN does not utilized data classification systems as IHGIN does not have the requirement to store classified information.		

Control ID	**MP-8(4)**	Control Name	**CLASSIFIED INFORMATION**
Definition	Downgrade system media containing classified information prior to release to individuals without required access authorizations.		
IHGIN Response	IHGIN does not utilized data classification systems as IHGIN does not have the requirement to store classified information.		

Physical and Environmental Protection

Control ID	**PE-1**	Control Name	**POLICY AND PROCEDURES**

Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] physical and environmental protection policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and c) Review and update the current physical and environmental protection: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	IHGIN employs strict physical and environmental protection to ensure the safety of data and staff employed at the IHGIN facility. IHGIN has strict policies and procedures to provide PCI compliant levels of physical security within the environment. Additionally physical security controls are put in place in order to protect sensitive raw materials from being manipulated or removed from the facility.

Control ID	**PE-2**	Control Name	**Physical Access Authorizations**
Definition	a) Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides; b) Issue authorization credentials for facility access c) Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and d) Remove individuals from the facility access list when access is no longer required		
IHGIN Response	IHGIN maintains an active list of staff and individuals that have access to the IHGIN facility. Access badges and credentials are issued		

Control ID	**PE-2(1)**	Control Name	**ACCESS BY POSITION AND ROLE**
Definition	Authorize physical access to the facility where the system resides based on position or role.		
IHGIN Response	IHGIN authorizes physical access based on role and specific user need.		

Control ID	**PE-2(2)**	Control Name	**TWO FORMS OF IDENTIFICATION**
Definition	Require two forms of identification from the following forms of identification for visitor access to the facility where the system resides: [Assignment: organization-defined list of acceptable forms of identification].		

IHGIN Response	IHGIN requires 2 forms of identification for visitor access to the facility.

Control ID	**PE-2(3)**	Control Name	**RESTRICT UNESCORTED ACCESS**
Definition	Restrict unescorted access to the facility where the system resides to personnel with [Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system; [Assignment: organization defined credentials]].		
IHGIN Response	Visitors and external contracts are prohibited from access to facilities without being escorted by an employee with access to said physical resource.		

Control ID	**PE-3**	Control Name	**Physical Access Control**
Definition	a) Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by: 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards]; b) Maintain physical access audit logs for [Assignment: organization-defined entry or exit points]; c) Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined controls]; d) Escort visitors and monitor visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and monitoring]; e) Secure keys, combinations, and other physical access devices; f) Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and g) Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.		
IHGIN Response	IHGIN enforces physical access control using audited badge access, mantraps, and magnetic locks. Access to public areas of the facility are locked and under badge access or an employee escorting the individual into the public area. Visitors are monitored and their access is logged. All secure badges are inventories and any change to access immediately renders the old access badge unusable.		

Control ID	**PE-3(1)**	Control Name	**SYSTEM ACCESS**
Definition	Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].		

IHGIN Response	The physical access control system is in the heart of the building behind several layers of physical security. Access to said system is monitored and changes are logged and reviewed by facilities staff prior to approval.

Control ID	**PE-3(2)**	Control Name	**FACILITY AND SYSTEM**
Definition	Perform security checks [Assignment: organization-defined frequency] at the physical perimeter of the facility or system for exfiltration of information or removal of system components.		
IHGIN Response	IHGIN performs external facility and perimeter checks to ensure that the exfiltration of systems or information cannot be achieved.		

Control ID	**PE-3(3)**	Control Name	**CONTINUOUS GUARDS**
Definition	Employ guards to control [Assignment: organization-defined physical access points] to the facility where the system resides 24 hours per day, 7 days per week.		
IHGIN Response	IHGIN utilized 24x7 video recording along with a security alarm that include window breaks, motion detection, and door access. The remote monitoring is conducted by a security team that can access video and report incidents directly to police. The monitored alarm system provides better security service that guarded access as guarded access is susceptible to being compromised by the guard themselves.		

Control ID	**PE-3(4)**	Control Name	**LOCKABLE CASINGS**
Definition	Use lockable physical casings to protect [Assignment: organization-defined system components] from unauthorized physical access.		
IHGIN Response	IHGIN uses lockable physical casings and cages to protect materials from potential misuse or theft.		

Control ID	**PE-3(5)**	Control Name	**TAMPER PROTECTION**
Definition	Employ [Assignment: organization-defined controls] to [Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the system.		
IHGIN Response	IHGIN asks that tamper protection is utilized within the supply chain to protect physical assets from tampering or alteration prior to usage within the facility.		

Control ID	**PE-3(6)**	Control Name	**FACILITY PENETRATION TESTING**
Definition	Deprecated (Implemented in CA-8)		
IHGIN Response	See response to CA-8		

Control ID	**PE-3(7)**	Control Name	**PHYSICAL BARRIERS**
Definition	Limit access using physical barriers.		
IHGIN Response	IHGIN uses iron mantraps and floor to ceiling fire coded walls to prevent access to the production floor by unauthorized individuals.		

Control ID	**PE-3(8)**	Control Name	**ACCESS CONTROL VESTIBULES**
Definition	Employ access control vestibules at [Assignment: organization-defined locations within the facility].		
IHGIN Response	IHGIN uses iron mantraps to prevent access to the production floor by unauthorized individuals.		

Control ID	**PE-4**	Control Name	**Access Control for Transmission**
Definition	Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].		
IHGIN Response	Transmission lines into the IHGIN facility utilize buried service to control physical access to the incoming connections.		

Control ID	**PE-5**	Control Name	**Access Control for Output Devices**
Definition	Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.		
IHGIN Response	Output devices are protected in the heart of the facility through multiple layers of badge access and video monitoring.		

Control ID	**PE-5(1)**	Control Name	**ACCESS TO OUTPUT BY AUTHORIZED INDIVIDUALS**
Definition	Deprecated (Implemented in PE-5)		
IHGIN Response	See response to PE-5		

Control ID	**PE-5(2)**	Control Name	**LINK TO INDIVIDUAL IDENTITY**
Definition	Link individual identity to receipt of output from output devices.		
IHGIN Response	IHGIN ensures that operators are logged into operator terminals and monitored on video to link output directly to the individual.		

Control ID	**PE-5(3)**	Control Name	**MARKING OUTPUT DEVICES**
Definition	Mark [Assignment: organization-defined system output devices] indicating the security marking of the types of information output from the device.		
IHGIN Response	Output devices such as printers mark the output to indicate the individual that sent the operation to the device. The exception being in license plate and registration production, the marking of the output takes place on the internal software side and isn't visually applied to the item.		

Control ID	**PE-6**	Control Name	**Monitoring Physical Access**
Definition	a) Monitor physical access to the facility where the system resides to detect and respond to physical security incidents; b) Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and		

	c) Coordinate results of reviews and investigations with the organizational incident response capability.
IHGIN Response	IHGIN utilized 24x7 video recording along with a security alarm that include window breaks, motion detection, and door access. The remote monitoring is conducted by a security team that can access video and report incidents directly to police and IHGIN staff. IHGIN staff review access logs periodically and the access logs are ingested into the IHGIN SIEM solution to monitor for any physical access that might be outside of the normal scope for a user.

Control ID	**PE-6(1)**	Control Name	**INTRUSION ALARMS AND SURVEILLANCE EQUIPMENT**
Definition	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.		
IHGIN Response	IHGIN utilized 24x7 video recording along with a security alarm that include window breaks, motion detection, and door access. The remote monitoring is conducted by a security team that can access video and report incidents directly to police and IHGIN staff.		

Control ID	**PE-6(2)**	Control Name	**AUTOMATED INTRUSION RECOGNITION AND RESPONSES**
Definition	Recognize [Assignment: organization-defined classes or types of intrusions] and initiate [Assignment: organization-defined response actions] using [Assignment: organization defined automated mechanisms].		
IHGIN Response	IHGIN monitoring will automatically alert a security monitoring organization upon the detection of an anomaly while enabled. The SIEM solution will alert IHGIT in the case that user access changes from the normally established baseline.		

Control ID	**PE-6(3)**	Control Name	**VIDEO SURVEILLANCE**
Definition	a) Employ video surveillance of [Assignment: organization-defined operational areas]; b) Review video recordings [Assignment: organization-defined frequency]; and c) Retain video recordings for [Assignment: organization-defined time-period].		
IHGIN Response	IHGIN utilized 24x7 video recording along with a security alarm that include window breaks, motion detection, and door access. The remote monitoring is conducted by a security team that can access video and report incidents directly to police and IHGIN staff. IHGIN will review video surveillance on occasion to ensure operation and in the case of any ongoing investigation.		

Control ID	**PE-6(4)**	Control Name	**MONITORING PHYSICAL ACCESS TO SYSTEMS**
Definition	Monitor physical access to the system in addition to the physical access monitoring of the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].		
IHGIN Response	Physical access to systems is audited and controlled using badge access. The system is monitored using the SIEM solution and access to the room the system is located in will alert IT when accessed in real-time.		

Control ID	**PE-7**	Control Name	**Visitor Control**
Definition	Deprecated (Implemented in PE-2 & PE-3)		
IHGIN Response	See response to PE-2 & PE-3		

Control ID	**PE-8**	Control Name	**Visitor Access Records**
Definition	a) Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time-period]; b) Review visitor access records [Assignment: organization-defined frequency]; and c) Report anomalies in visitor access records to [Assignment: organization-defined personnel].		
IHGIN Response	IHGIN maintains visitor access records and reviews them to ensure that no anomalous behavior occurs.		

Control ID	**PE-8(1)**	Control Name	**AUTOMATED RECORDS MAINTENANCE AND REVIEW**
Definition	Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	IHGIN systems ingest visitor access audit logs and monitor access for anomalous behavior and will alert IT to any potential issues.		

Control ID	**PE-8(2)**	Control Name	**PHYSICAL ACCESS RECORDS**
Definition	Deprecated (Implemented in PE-2)		
IHGIN Response	See response to PE-2		

Control ID	**PE-9**	Control Name	**Power Equipment and Cabling**
Definition	Protect power equipment and power cabling for the system from damage and destruction.		
IHGIN Response	Power equipment and cabling is installed professional in compliance with local regulations and laws.		

Control ID	**PE-9(1)**	Control Name	**REDUNDANT CABLING**
Definition	Employ redundant power cabling paths that are physically separated by [Assignment: organization-defined distance].		
IHGIN Response	IHGIN has redundant power cabling run into the production floor on multiple circuits to ensure that systems are physically separated. The cabling was professionally installed into protective conduit and is distanced to provide redundancy where required.		

Control ID	**PE-9(2)**	Control Name	**AUTOMATIC VOLTAGE CONTROLS**
Definition	Employ automatic voltage controls for [Assignment: organization-defined critical system components].		

IHGIN Response	IHGIN utilizes voltage regulators to ensure that voltage remains within control.

Control ID	**PE-10**	Control Name	**Emergency Shutoff**
Definition	a) Provide the capability of shutting off power to [Assignment: organization-defined system or individual system components] in emergency situations; b) Place emergency shutoff switches or devices in [Assignment: organization-defined location by system or system component] to facilitate access for authorized personnel; and c) Protect emergency power shutoff capability from unauthorized activation.		
IHGIN Response	IHGIN has an emergency power shutoff located in the electrical room. Only authorized individual have access to the emergency power shutoff.		

Control ID	**PE-10(1)**	Control Name	**ACCIDENTAL AND UNAUTHORIZED ACTIVATION**
Definition	Deprecated (Implemented in PE-10)		
IHGIN Response	See response to PE-10		

Control ID	**PE-11**	Control Name	**Emergency Power**
Definition	Provide an uninterruptible power supply to facilitate [Selection (one or more): an orderly shutdown of the system; transition of the system to long-term alternate power] in the event of a primary power source loss.		
IHGIN Response	IHGIN utilizes a ups to provide power in the case primary power loss.		

Control ID	**PE-11(1)**	Control Name	**ALTERNATE POWER SUPPLY — MINIMAL OPERATIONAL CAPABILITY**
Definition	Provide an alternate power supply for the system that is activated [Selection: manually; automatically] and that can maintain minimally required operational capability in the event of an extended loss of the primary power source.		
IHGIN Response	IHGIN backup power has been able to provide power to the facility through every power interruption experienced at the facility to date.		

Control ID	**PE-11(2)**	Control Name	**ALTERNATE POWER SUPPLY — SELF-CONTAINED**
Definition	Provide an alternate power supply for the system that is activated [Selection: manually; automatically] and that is: a) Self-contained; b) Not reliant on external power generation; and c) Capable of maintaining [Selection: minimally required operational capability; full operational capability] in the event of an extended loss of the primary power source.		

IHGIN Response	IHGIN backup power is self-contained, and not reliant on external power generation. It has been able to provide backup power to the facility through every power interruption experienced to date.

Control ID	**PE-12**	Control Name	**Emergency Lighting**
Definition	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.		
IHGIN Response	IHGIN maintains battery powered emergency lighting to all areas of the facility in the case that power goes down.		

Control ID	**PE-12(1)**	Control Name	**ESSENTIAL MISSIONS AND BUSINESS FUNCTIONS**
Definition	Provide emergency lighting for all areas within the facility supporting essential missions and business functions		
IHGIN Response	IHGIN maintains battery powered emergency lighting to all areas of the facility in the case that power goes down.		

Control ID	**PE-13**	Control Name	**Fire Protection**
Definition	Employ and maintain fire detection and suppression systems that are supported by an independent energy source		
IHGIN Response	IHGIN utilized fire detection and suppression systems that are supported by battery backup.		

Control ID	**PE-13(1)**	Control Name	**DETECTION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION**
Definition	Employ fire detection systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders] in the event of a fire.		
IHGIN Response	IHGIN fire detection systems automatically notify the appropriate authorities in the case of a fire being detected.		

Control ID	**PE-13(2)**	Control Name	**SUPPRESSION SYSTEMS — AUTOMATIC ACTIVATION AND NOTIFICATION**
Definition	a) Employ fire suppression systems that activate automatically and notify [Assignment: organization-defined personnel or roles] and [Assignment: organization-defined emergency responders]; and b) Employ an automatic fire suppression capability when the facility is not staffed on a continuous basis.		
IHGIN Response	IHGIN fire sprinkler systems activate automatically and notify the appropriate authorities regardless of the time of day or how many individuals are in the building.		

Control ID	**PE-13(3)**	Control Name	**AUTOMATIC FIRE SUPPRESSION**
Definition	Deprecated (Implemented in PE-13(2))		

IHGIN Response	See response to PE-13(2)

Control ID	**PE-13(4)**	Control Name	**INSPECTIONS**
Definition	Ensure that the facility undergoes [Assignment: organization-defined frequency] fire protection inspections by authorized and qualified inspectors and identified deficiencies are resolved within [Assignment: organization-defined time-period].		
IHGIN Response	IHGIN ensures that all personnel protection systems are inspected and maintained according to local regulations.		

Control ID	**PE-14**	Control Name	**Environmental Controls**
Definition	a) Maintain [Selection (one or more): temperature; humidity; pressure; radiation; [Assignment: organization-defined environmental control]] levels within the facility where the system resides at [Assignment: organization-defined acceptable levels]; and b) Monitor environmental control levels [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN maintains and monitors environment controls around temperature, humidity, and gas systems. Environmental controls are closely monitored to remain within the tolerance levels outlined by our materials manufacturers.		

Control ID	**PE-14(1)**	Control Name	**AUTOMATIC CONTROLS**
Definition	Employ the following automatic environmental controls in the facility to prevent fluctuations potentially harmful to the system: [Assignment: organization-defined automatic environmental controls].		
IHGIN Response	IHGIN systems will automatically take actions in the case of environment controls being outside of tolerance levels.		

Control ID	**PE-14(2)**	Control Name	**MONITORING WITH ALARMS AND NOTIFICATIONS**
Definition	Employ environmental control monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment to [Assignment: organization defined personnel or roles].		
IHGIN Response	IHGIN IT monitors environmental controls and will receive alarms and notifications if environmental controls go outside of predefined tolerance levels.		

Control ID	**PE-15**	Control Name	**Water Damage Protection**
Definition	Protect the system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.		
IHGIN Response	IHGIN facility has a master shutoff value and isolation valves that are working properly and known to key personnel.		

Control ID	**PE-15(1)**	Control Name	**AUTOMATION SUPPORT**

Definition	Detect the presence of water near the system and alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms].
IHGIN Response	IHGIN systems perform this check and alerting function.

Control ID	**PE-16**	Control Name	**Delivery and Removal**
Definition	a) Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; and b) Maintain records of the system components		
IHGIN Response	IHGIN controls all systems and components within the facility and maintains records of systems maintenance on components within.		

Control ID	**PE-17**	Control Name	**Alternate Work Site**
Definition	a) Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees; b) Employ the following controls at alternate work sites: [Assignment: organization-defined controls]; c) Assess the effectiveness of controls at alternate work sites; and d) Provide a means for employees to communicate with information security and privacy personnel in case of incidents		
IHGIN Response	IHGIN has a predefined alternate work site established in the case an issue occurs at the IHGIN facility. The alternate worksite has a similar level of physical access and environmental controls in place.		

Control ID	**PE-18**	Control Name	**Location of System Components**
Definition	Position system components within the facility to minimize potential damage from [Assignment: organization-defined physical and environmental hazards] and to minimize the opportunity for unauthorized access.		
IHGIN Response	IHGIN places system components in locked areas protected by badge access to prevent damage from unauthorized access.		

Control ID	**PE-18(1)**	Control Name	**FACILITY SITE**
Definition	Deprecated (Implemented in PE-23)		
IHGIN Response	See response to PE-23		

Control ID	**PE-19**	Control Name	**Information Leakage**
Definition	Protect the system from information leakage due to electromagnetic signals emanations.		
IHGIN Response	IHGIN does not utilize faraday cages, but does ensure that data transmission lines are not located within close proximity to shielded exterior walls that could potentially lead to electromagnetic emanation.		

Control ID	**PE-19(1)**	Control Name	**NATIONAL EMISSIONS AND TEMPEST POLICIES AND PROCEDURES**
Definition	Protect system components, associated data communications, and networks in accordance with national Emissions Security policies and procedures based on the security category or classification of the information.		
IHGIN Response	IHGIN does not house classified information.		

Control ID	**PE-20**	Control Name	**Asset Monitoring and Tracking**
Definition	Employ [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].		
IHGIN Response	IHGIN monitors and tracks all assets within the organization.		

Control ID	**PE-21**	Control Name	**Electromagnetic Pulse Protection**
Definition	Employ [Assignment: organization-defined controls] against electromagnetic pulse damage for [Assignment: organization-defined systems and system components].		
IHGIN Response	IHGIN uses surge suppressors and shielding on critical systems where applicable and safe to do so.		

Control ID	**PE-22**	Control Name	**Component Marking**
Definition	Mark [Assignment: organization-defined system hardware components] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.		
IHGIN Response	IHGIN does not process classified information.		

Control ID	**PE-23**	Control Name	**Facility Location**
Definition	a) Plan the location or site of the facility where the system resides considering physical and environmental hazards; and b) For existing facilities, consider the physical and environmental hazards in the organizational risk management strategy.		
IHGIN Response	IHGIN has conducted a site assessment to ensure that all risk involving natural hazards and physical access has been considered. This information is considered within the organizational risk management strategy.		

Planning Family

Control ID	**PL-1**	Control Name	**POLICY AND PROCEDURES**

Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] planning policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the planning policy and the associated planning controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and c) Review and update the current planning: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	IHGIN IT maintains an IT strategy that allows the organization to create IT policies and procedures using risk management in order to facilitate the achievement of organizational business goals while ensuring that customer data remains secure.

Control ID	**PL-2**	Control Name	**System Security and Privacy Plans**
Definition	a) Develop security and privacy plans for the system that: 1. Are consistent with the organization's enterprise architecture; 2. Explicitly define the constituent system components; 3. Describe the operational context of the system in terms of missions and business processes; 4. Provide the security categorization of the system, including supporting rationale; 5. Describe any specific threats to the system that are of concern to the organization; 6. Provide the results of a privacy risk assessment for systems processing personally identifiable information; 7. Describe the operational environment for the system and any dependencies on or connections to other systems or system components; 8. Provide an overview of the security and privacy requirements for the system; 9. Identify any relevant control baselines or overlays, if applicable; 10. Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions; 11. Include risk determinations for security and privacy architecture and design decisions; 12. Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and		

	13. Are reviewed and approved by the authorizing official or designated representative prior to plan implementation. b) Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles]; c) Review the plans [Assignment: organization-defined frequency]; d) Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and e) Protect the plans from unauthorized disclosure and modification.
IHGIN Response	IHGIN IT has a Security Policy that contains the organizational policies and procedures as it pertains to IT Security and Data Privacy.

Control ID	**PL-2(1)**	Control Name	**CONCEPT OF OPERATIONS**
Definition	Deprecated (Implemented in PL-7)		
IHGIN Response	See response to PL-7		

Control ID	**PL-2(2)**	Control Name	**FUNCTIONAL ARCHITECTURE**
Definition	Deprecated (Implemented in PL-8)		
IHGIN Response	See response to PL-8		

Control ID	**PL-2(3)**	Control Name	**PLAN AND COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES**
Definition	Deprecated (Implemented in PL-2)		
IHGIN Response	See response to PL-2		

Control ID	**PL-3**	Control Name	**System Security Plan Update**
Definition	Deprecated (Implemented in PL-2)		
IHGIN Response	See response to PL-2		

Control ID	**PL-4**	Control Name	**Rules of Behavior**
Definition	a) Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy; b) Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system; c) Review and update the rules of behavior [Assignment: organization-defined frequency]; and		

	d) Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].
IHGIN Response	IHGIN has an acceptable usage policy that staff are required to review and sign off on prior to beginning work.

Control ID	**PL-4(1)**	Control Name	**SOCIAL MEDIA AND EXTERNAL SITE/APPLICATION USAGE RESTRICTIONS**
Definition	Include in the rules of behavior, restrictions on: a) Use of social media, social networking sites, and external sites/applications; b) Posting organizational information on public websites; and c) Use of organization-provided credentials (i.e., email addresses) for creating accounts on external sites/applications.		
IHGIN Response	IHGIN disallows staff from posting private customer or business information on social media. IHGIN does not restrict speech of staff, but on social media sites where staff identify their employer, they are to maintain a professional posture.		

Control ID	**PL-5**	Control Name	**Privacy Impact Assessment**
Definition	Deprecated (Implemented in RA-8)		
IHGIN Response	See response to RA-8		

Control ID	**PL-6**	Control Name	**Security-Related Activity Planning**
Definition	Deprecated (Implemented in PL-2)		
IHGIN Response	See response to PL-2		

Control ID	**PL-7**	Control Name	**Concept of Operations**
Definition	a) Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and b) Review and update the CONOPS [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN develops CONOPS for internal process mapping and software creation.		

Control ID	**PL-8**	Control Name	**Security and Privacy Architectures**
Definition	a) Develop security and privacy architectures for the system that: 1. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information; 2. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;		

	3. Describe how the architectures are integrated into and support the enterprise architecture; and 4. Describe any assumptions about, and dependencies on, external systems and services; b) Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and c) Reflect planned architecture changes in the security and privacy plans, the Concept of Operations (CONOPS), organizational procedures, and procurements and acquisitions.
IHGIN Response	The IHGIN Enterprise Architect designs systems with CONOPS in mind in order to ensure that the CIA triad is maintained.

Control ID	**PL-8(1)**	Control Name	**DEFENSE-IN-DEPTH**
Definition	Design the security and privacy architectures for the system using a defense-in-depth approach that: a) Allocates [Assignment: organization-defined controls] to [Assignment: organization defined locations and architectural layers]; and b) Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.		
IHGIN Response	IHGIN deploys controls that employ the onion model of defense in depth. From firewall through to local intrusion detection and prevention, all systems are monitored to ensure that the organizational security posture remains alerts.		

Control ID	**PL-8(2)**	Control Name	**SUPPLIER DIVERSITY**
Definition	Require that [Assignment: organization-defined controls] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.		
IHGIN Response	IHGIN utilizes several different security vendors within the environment in order to ensure that the organization is protected.		

Control ID	**PL-9**	Control Name	**Central Management**
Definition	Centrally manage [Assignment: organization-defined controls and related processes].		
IHGIN Response	All server and network infrastructure is centrally managed.		

Control ID	**PL-10**	Control Name	**Baseline Selection**
Definition	Select a control baseline for the system		
IHGIN Response	IHGIN uses an adaptive baseline that allows the SIEM solution to apply machine learning to user actions to determine if they are normal or outside of the norm.		

Control ID	**PL-11**	Control Name	**Baseline Tailoring**
Definition	Tailor the selected control baseline by applying specified tailoring actions.		

IHGIN Response	IHGIN uses an adaptive baseline that allows the SIEM solution to apply machine learning to user actions to determine if they are normal or outside of the norm.

Program Management

Control ID	**PM-1**	Control Name	**Information Security Program Plan**
Definition	a) Develop and disseminate an organization-wide information security program plan that: 1. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; 2. Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 3. Reflects the coordination among organizational entities responsible for information security; and 4. Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; b) Review the organization-wide information security program plan [Assignment: organization defined frequency]; c) Update the information security program plan to address organizational changes and problems identified during plan implementation or control assessments; and d) Protect the information security program plan from unauthorized disclosure and modification.		
IHGIN Response	IHGIN maintains the information security plan as part of the strategic plan for IHGIN IT. This outlines the plan for implementation of controls and systems to improve security posture and react to newly discovered cyber risks. The IHGIN security plan utilizes the NIST SP 800-53 revision 5 to ensure that the latest controls have been considered.		

Control ID	**PM-2**	Control Name	**Information Security Program Leadership Role**
Definition	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.		
IHGIN Response	The IHGIN Enterprise Architect is responsible for coordinating the resources and systems to achieve the mission of the plan.		

Control ID	**PM-3**	Control Name	**Information Security and Privacy Resources**
Definition	a) Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement; b) Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance		

	with applicable laws, executive orders, directives, policies, regulations, standards; and c) Make available for expenditure, the planned information security and privacy resources.
IHGIN Response	IHGIN establishes the resources and requirements for each control when at the time of the control being implemented. An estimation is provided in the strategic plan that outlines the future vision for IHGIN, however at the time of the project charter being developed the official budget and resources are allocated.

Control ID	**PM-4**	Control Name	**Plan of Action and Milestones Proces**
Definition	a) Implement a process to ensure that plans of action and milestones for the information security and privacy programs and associated organizational systems: 1. Are developed and maintained; 2. Document the remedial information security and privacy actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and 3. Are reported in accordance with established reporting requirements. b) Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.		
IHGIN Response	IHGIN IT maintains project management procedures that ensure that a plan of action is documented for each item within the strategic plan and at the time of project kickoff the milestones for the project are defined along with a risk register.		

Control ID	**PM-5**	Control Name	**System Inventory**
Definition	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.		
IHGIN Response	IHGIN maintains an up to date inventory of systems.		

Control ID	**PM-5(1)**	Control Name	**INVENTORY OF PERSONALLY IDENTIFIABLE INFORMATION**
Definition	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.		
IHGIN Response	The systems that contain PII are clearly identified by IHGIN and the inventory of these systems is maintained.		

Control ID	**PM-6**	Control Name	**Measures of Performance**
Definition	Develop, monitor, and report on the results of information security and privacy measures of performance		
IHGIN Response	IHGIN measures performance based on a return on risk and reportable metrics provided by controls that have been implemented to mitigate risk.		

Control ID	**PM-7**	Control Name	**Enterprise Architecture**
Definition	Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.		
IHGIN Response	IHGIN has an enterprise architect that has developed an enterprise architecture plan.		

Control ID	**PM-7(1)**	Control Name	**OFFLOADING**
Definition	Offload [Assignment: organization-defined non-essential functions or services] to other systems, system components, or an external provider		
IHGIN Response	IHGIN IT currently does not offload services at the Indiana facility to external third parties.		

Control ID	**PM-8**	Control Name	**Critical Infrastructure Plan**
Definition	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.		
IHGIN Response	IT has established a clear definition of the critical infrastructure within the organization and put controls in place to ensure that critical infrastructure is protected. There is currently no defined critical infrastructure plan, as much as the information is defined within the IHGIN Security Policy and systems architecture documents.		

Control ID	**PM-9**	Control Name	**Risk Management Strategy**
Definition	a) Develops a comprehensive strategy to manage: 1. Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and 2. Privacy risk to individuals resulting from the authorized processing of personally identifiable information; b) Implement the risk management strategy consistently across the organization; and c) Review and update the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.		
IHGIN Response	IT maintains a risk register for each project and has an internal risk management strategy for both IT and business operations.		

Control ID	**PM-10**	Control Name	**Authorization Process**
Definition	a) Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes; b) Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and c) Integrate the authorization processes into an organization-wide risk management program.		
IHGIN Response	Internally authorization for procedure on risk related items is up to the President and Vice President of the organization.		

Control ID	**PM-11**	Control Name	**Mission and Business Process Definition**
Definition	a) Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and b) Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and c) Review and revise the mission and business processes [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN has clear definitions for business processes in place to ensure that handling of PII is done with the understanding of the potential risks associated with that information.		

Control ID	**PM-12**	Control Name	**Insider Threat Program**
Definition	Implement an insider threat program that includes a cross-discipline insider threat incident handling team.		
IHGIN Response	IHGIN Management is responsible for reporting any potential insider threats to the organization. Staff levels of job satisfaction are measured at regular intervals to help maintain a positive work environment that won't lead to a potential insider threat.		

Control ID	**PM-13**	Control Name	**Security and Privacy Workforce**
Definition	Establish a security and privacy workforce development and improvement program.		
IHGIN Response	IHGIN IT has undertaken a security and privacy workforce development and improvement program.		

Control ID	**PM-14**	Control Name	**Testing, Training, and Monitoring**
Definition	a) Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems: 1. Are developed and maintained; and 2. Continue to be executed; and b) Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.		
IHGIN Response	IT staff will randomly test staff during their normal day to day operations to ensure that users are complying with internal policies and procedures. If a user fails the test they are required to take training at the time of incident prior to gaining network access again.		

Control ID	**PM-15**	Control Name	**Security and Privacy Groups and Associations**
Definition	Establish and institutionalize contact with selected groups and associations within the security and privacy communities: a) To facilitate ongoing security and privacy education and training for organizational personnel;		

	b) To maintain currency with recommended security and privacy practices, techniques, and technologies; and c) To share current security and privacy information, including threats, vulnerabilities, and incidents.
IHGIN Response	The IHGIN Enterprise Architect maintains organizational membership with ISACA and ISC2. The information provided to the EA from these organizations is used in creating internal training documentation and content.

Control ID	**PM-16**	Control Name	**Threat Awareness Program**
Definition	Implement a threat awareness program that includes a cross-organization information sharing capability for threat intelligence.		
IHGIN Response	IHGIN asks staff to actively share potential threats and news stories with IT staff. This is done as a function to get employees more involved in enterprise security and to gain an understanding of what threats are out there. IT staff also provide regular training to staff on potential threats to the organization and safe browsing habits to use at both the office and at home.		

Control ID	**PM-16(1)**	Control Name	**AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE**
Definition	Employ automated mechanisms to maximize the effectiveness of sharing threat intelligence information.		
IHGIN Response	Internally IT staff receive automated threat notifications from third party vendors and monitor system for potential vulnerabilities.		

Control ID	**PM-17**	Control Name	**Protecting CUI on External Systems**
Definition	a) Establish policy and procedures to ensure that requirements for the protection of controlled unclassified information that is processed, stored or transmitted on external systems, are implemented in accordance with applicable laws, executive orders, directives, policies, regulations, and standards. b) Update the policy and procedures [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN does not house classified information. This has not been implemented at this time.		

Control ID	**PM-18**	Control Name	**Privacy Program Plan**
Definition	a) Develop and disseminate an organization-wide privacy program plan that provides an overview of the agency's privacy program, and: 1. Includes a description of the structure of the privacy program and the resources dedicated to the privacy program; 2. Provides an overview of the requirements for the privacy program and a description of the privacy program management controls and common controls in place or planned for meeting those requirements;		

	3. Includes the role of the senior agency official for privacy and the identification and assignment of roles of other privacy officials and staff and their responsibilities; 4. Describes management commitment, compliance, and the strategic goals and objectives of the privacy program; 5. Reflects coordination among organizational entities responsible for the different aspects of privacy; and 6. Is approved by a senior official with responsibility and accountability for the privacy risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation; and b) Update the plan to address changes in federal privacy laws and policy and organizational changes and problems identified during plan implementation or privacy control assessments.
IHGIN Response	The organization utilized the Security Policy, Security Plan, Acceptable Usage Policy, and Employee Handbook to achieve this function. Privacy is an integral part of all aspects of the business and thus the importance of maintaining it is repeated across multiple policies and documents.

Control ID	**PM-19**	Control Name	**Privacy Program Leadership Role**
Definition	Appoint a senior agency official for privacy with the authority, mission, accountability, and resources to coordinate, develop, and implement, applicable privacy requirements and manage privacy risks through the organization-wide privacy program.		
IHGIN Response	IHGIN recognizes the importance of privacy and thus the President of the organization is responsible for the privacy program. Portions of the program are assigned to each functional manager to implement.		

Control ID	**PM-20**	Control Name	**Dissemination of Privacy Program Information**
Definition	Maintain a central resource webpage on the organization's principal public website that serves as a central source of information about the organization's privacy program and that: a) Ensures that the public has access to information about organizational privacy activities and can communicate with its senior agency official for privacy; b) Ensures that organizational privacy practices and reports are publicly available; and c) Employs publicly facing email addresses and/or phone lines to enable the public to provide feedback and/or direct questions to privacy offices regarding privacy practices		
IHGIN Response	IHGIN maintains important information pertaining to the Privacy Program and all other business initiatives on the corporate intranet.		

Control ID	**PM-21**	Control Name	**Accounting of Disclosures**
Definition	a) Develop and maintain an accurate accounting of disclosures of personally identifiable information, including: 1. Date, nature, and purpose of each disclosure; and		

	2. Name and address, or other contact information of the person or organization to which the disclosure was made; b) Retain the accounting of disclosures for the length of the time the personally identifiable information is maintained or five years after the disclosure is made, whichever is longer; and c) Make the accounting of disclosures available to the individual to whom the personally identifiable information relates upon request.
IHGIN Response	PII is not to be disclosed to a third party external to the organization at any time. In the case that the customer asks for their data that requires is logged and signed off on by both parties prior to disclosure.

Control ID	**PM-22**	Control Name	**Personally Identifiable Information Quality Management**
Definition	Develop and document policies and procedures for: a) Reviewing for the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle; b) Correcting or deleting inaccurate or outdated personally identifiable information; c) Disseminating notice of corrected or deleted personally identifiable information to individuals or other appropriate entities; and d) Appeals of adverse decisions on correction or deletion requests.		
IHGIN Response	IHGIN does not edit customer data without expressed consent of the customer. PII is not changes after being ingested into iPrime or any other IHGIN system.		

Control ID	**PM-23**	Control Name	**Data Governance Body**
Definition	Establish a Data Governance Body consisting of [Assignment: organization-defined roles] with [Assignment: organization-defined responsibilities].		
IHGIN Response	IHGIN has a data governance body including the Enterprise Architect, VP of Finance, and Customer Service Manager.		

Control ID	**PM-24**	Control Name	**Data Integrity Board**
Definition	Establish a Data Integrity Board to: a) Review proposals to conduct or participate in a matching program; and b) Conduct an annual review of all matching programs in which the agency has participated.		
IHGIN Response	IHGIN does not have a data integrity board, the governance team and IT are responsible for maintaining integrity of data.		

Control ID	**PM-25**	Control Name	**Minimization of PII Used in Testing Training, and Research**
Definition	a) Develop, document, and implement policies and procedures that address the use of personally identifiable information for internal testing, training, and research; b) Limit or minimize the amount of personally identifiable information used for internal testing, training, and research purposes;		

	c) Authorize the use of personally identifiable information when such information is required for internal testing, training, and research; and d) Review and update policies and procedures [Assignment: organization-defined frequency].
IHGIN Response	In testing, real PII is not used. IHGIN maintains an active list of example files that customers regularly send to IHGIN. These samples are used in testing and training.

Control ID	**PM-26**	Control Name	**Complaint Management**
Definition	Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the organizational privacy practices that includes: a) Mechanisms that are easy to use and readily accessible by the public; b) All information necessary for successfully filing complaints; c) Tracking mechanisms to ensure all complaints received are reviewed and addressed within [Assignment: organization-defined time-period]; d) Acknowledgement of receipt of complaints, concerns, or questions from individuals within [Assignment: organization-defined time-period]; and e) Response to complaints, concerns, or questions from individuals within [Assignment: organization-defined time-period].		
IHGIN Response	Customer Service is responsible for processing and responding to all customer complaints, concerns, or questions and tracking them through to resolution.		

Control ID	**PM-27**	Control Name	**Privacy Reporting**
Definition	a) Develop [Assignment: organization-defined privacy reports] and disseminate to: 1. OMB, Congress, and other oversight bodies to demonstrate accountability with statutory, regulatory, and policy privacy mandates; and 2. [Assignment: organization-defined officials] and other personnel with responsibility for monitoring privacy program compliance; and b) Review and update privacy reports [Assignment: organization-defined frequency].		
IHGIN Response	The Enterprise Architect is responsible for reporting on changes to privacy legislation that impacts customer data and adjusting controls in order to meet any new regulations.		

Control ID	**PM-28**	Control Name	**Risk Framing**
Definition	a) Identify and document: 1. Assumptions affecting risk assessments, risk responses, and risk monitoring; 2. Constraints affecting risk assessments, risk responses, and risk monitoring; 3. Priorities and trade-offs considered by the organization for managing risk; and 4. Organizational risk tolerance; and b) Distribute the results of risk framing activities to [Assignment: organization-defined personnel];		

	c) Review and update risk framing considerations [Assignment: organization-defined frequency].
IHGIN Response	Risk framing is conducted at the organizational level. The assumptions, constraints, risk tolerance, priorities, and tradeoffs are identified internally when conducting risk framing activities. This informs management decisions around implementation of new business processes, systems, and controls.

Control ID	**PM-29**	Control Name	**Risk Management Program Leadership Roles**
Definition	a) Appoint a Senior Accountable Official for Risk Management to align organizational information security and privacy management processes with strategic, operational, and budgetary planning processes; and b) Establish a Risk Executive (function) to view and analyze risk from an organization-wide perspective and ensure management of risk is consistent across the organization.		
IHGIN Response	The Enterprise Architect serves this role.		

Control ID	**PM-30**	Control Name	**Supply Chain Risk Management Strategy**
Definition	a) Develop an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services; b) Implement the supply chain risk management strategy consistently across the organization; and c) Review and update the supply chain risk management strategy on [Assignment: organization-defined frequency] or as required, to address organizational changes.		
IHGIN Response	Supply chain risks are reviewed internally and the organization has a risk management strategy in place to manage supply chain risk.		

Control ID	**PM-31**	Control Name	**Continuous Monitoring Strategy**
Definition	Develop an organization-wide continuous monitoring strategy and implement continuous monitoring programs that include: a) Establishing the following organization-wide metrics to be monitored: [Assignment: organization-defined metrics]; b) Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness; c) Ongoing monitoring of organizationally-defined metrics in accordance with the continuous monitoring strategy; d) Correlation and analysis of information generated by control assessments and monitoring; e) Response actions to address results of the analysis of control assessment and monitoring information; and		

	f) Reporting the security and privacy status of organizational systems to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].
IHGIN Response	IT monitors all systems and metrics to ensure that they are not outside of the baselined data.

Control ID	**PM-32**	Control Name	**Purposing**
Definition	Analyze [Assignment: organization-defined systems or systems components] supporting mission essential services or functions to ensure that the information resources are being used consistent with their intended purpose		
IHGIN Response	All business processes and systems are reviewed to ensure that they are being used for their designed purpose.		

Control ID	**PM-33**	Control Name	**Privacy Policies on Websites, Applications, and Digital Services**
Definition	Develop and post privacy policies on all external-facing websites, mobile applications, and other digital services, that: a) Are written in plain language and organized in a way that is easy to understand and navigate; b) Provide useful information that the public would need to make an informed decision about whether and how to interact with the organization; and c) Are updated whenever the organization makes a substantive change to the practices it describes and includes a time/date stamp to inform the public of the date of the most recent changes.		
IHGIN Response	The website does not have a privacy policy published on it at this time. The IHGIN website does not accept confidential information from users or track their usage outside of the website. There is no legal requirement to do this at this time, if a new regulation introduces the requirement or a customer requests that it be implemented it can be done easily.		

Personnel Security

Control ID	**PS-1**	Control Name	**POLICY AND PROCEDURES**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] personnel security policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;		

	b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and c) Review and update the current personnel security: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	IHGIN has internal policies established for staffing actions and personnel security of employees and contractors. This information is contained in the employee handbook and on-site contractor policies.

Control ID	**PS-2**	Control Name	**Position Risk Designation**
Definition	a) Assign a risk designation to all organizational positions; b) Establish screening criteria for individuals filling those positions; and c) Review and update position risk designations [Assignment: organization-defined frequency].		
IHGIN Response	Risk designation is considered when calculating organizational salary levels for various positions. A risk designation is assigned to each position and criteria required to fill the position is identified.		

Control ID	**PS-3**	Control Name	**Personnel Screening**
Definition	a) Screen individuals prior to authorizing access to the system; and b) Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].		
IHGIN Response	All staff are required to be screened for criminal record checks and references prior to being employed.		

Control ID	**PS-3(1)**	Control Name	**CLASSIFIED INFORMATION**
Definition	Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.		
IHGIN Response	IHGIN does not currently house classified information. There is currently no plan to implement the screening criteria required for access secret or top-secret information.		

Control ID	**PS-3(2)**	Control Name	**FORMAL INDOCTRINATION**
Definition	Verify that individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.		
IHGIN Response	IHGIN does not currently house classified information. There is currently no plan to implement the screening criteria required for access secret or top-secret information.		

Control ID	**PS-3(3)**	Control Name	**INFORMATION WITH SPECIAL PROTECTION MEASURES**

Definition	Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection: a) Have valid access authorizations that are demonstrated by assigned official government duties; and b) Satisfy [Assignment: organization-defined additional personnel screening criteria].
IHGIN Response	Currently IHGIN does not house information or data with special protection measures in place. If required IHGIN can facilitate having staff more through authorization procedures if required.

Control ID	**PS-3(4)**	Control Name	**CITIZENSHIP REQUIREMENTS**
Definition	Verify that individuals accessing a system processing, storing, or transmitting [Assignment: organization-defined information types] meet [Assignment: organization-defined citizenship requirements].		
IHGIN Response	IHGIN requires that staff accessing systems have citizenship from a NATO allied nation.		

Control ID	**PS-4**	Control Name	**Personnel Termination**
Definition	a) Disable system access within [Assignment: organization-defined time-period]; b) Terminate or revoke any authenticators and credentials associated with the individual; c) Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics]; d) Retrieve all security-related organizational system-related property; and e) Retain access to organizational information and systems formerly controlled by terminated individual.		
IHGIN Response	All systems access for users is documented by IT and access it terminated at the time of termination. Information and systems used by the terminated individual are backed up and maintained by the organization.		

Control ID	**PS-4(1)**	Control Name	**POST-EMPLOYMENT REQUIREMENTS**
Definition	a) Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and b) Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.		
IHGIN Response	Terminated employees are reminded of their legally binding obligations and non-disclosure/non-complete requirements.		

Control ID	**PS-4(2)**	Control Name	**AUTOMATED NOTIFICATION**
Definition	Notify [Assignment: organization-defined personnel or roles] of individual termination actions using [Assignment: organization-defined automated mechanisms]		
IHGIN Response	Notification of termination is not automated as the request to block systems access is typically done prior to termination. In the case that a manager or individual responsible for conducting termination procedures were to be terminated the automated		

	notification could potentially allow them to cause undue harm to the organization prior to being escorted from the facility.

Control ID	**PS-5**	Control Name	**Personnel Transfer**
Definition	a) Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization; b) Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time-period following the formal transfer action]; c) Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and d) Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time-period].		
IHGIN Response	At the time of personnel transfer all logistics and requirements are coordinated between IT and HR.		

Control ID	**PS-6**	Control Name	**Access Agreements**
Definition	a) Develop and document access agreements for organizational systems; b) Review and update the access agreements [Assignment: organization-defined frequency]; and c) Verify that individuals requiring access to organizational information and systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].		
IHGIN Response	All users are required to sign an acceptable usage policy and understand the IHGIN Security Policy prior to being given network access.		

Control ID	**PS-6(1)**	Control Name	**INFORMATION REQUIRING SPECIAL PROTECTION**
Definition	Deprecated (Implemented in PS-3)		
IHGIN Response	See response to PS-3		

Control ID	**PS-6(2)**	Control Name	**CLASSIFIED INFORMATION REQUIRING SPECIAL PROTECTION**
Definition	Verify that access to classified information requiring special protection is granted only to individuals who: a) Have a valid access authorization that is demonstrated by assigned official government duties; b) Satisfy associated personnel security criteria; and c) Have read, understood, and signed a nondisclosure agreement.		

IHGIN Response	IHGIN does not currently house classified information. There is currently no plan to implement the screening criteria required for access secret or top-secret information.

Control ID	**PS-6(3)**	Control Name	**POST-EMPLOYMENT REQUIREMENTS**
Definition	a) Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and b) Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.		
IHGIN Response	Terminated employees are reminded of their legally binding obligations and non-disclosure/non-complete requirements.		

Control ID	**PS-7**	Control Name	**External Personnel Security**
Definition	a) Establish personnel security requirements, including security roles and responsibilities for external providers; b) Require external providers to comply with personnel security policies and procedures established by the organization; c) Document personnel security requirements; d) Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization defined time-period]; and e) Monitor provider compliance with personnel security requirements.		
IHGIN Response	External contractors and users are required to understand the IHGIN contractor policy prior to being given access to any systems or data.		

Control ID	**PS-8**	Control Name	**Personnel Sanctions**
Definition	a) Employ a formal sanctions process for individuals failing to comply with established information security and privacy policies and procedures; and b) Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time-period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.		
IHGIN Response	IHGIN IT Acceptable Usage and Security policies highlights potential sanctions for non-compliance with the policy.		

PII Processing and Transparency

Control ID	**PT-1**	Control Name	**Policy and Procedures**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] personally identifiable information processing and transparency policy that:		

	a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the personally identifiable information processing and transparency policy and the associated personally identifiable information processing and transparency controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident personally identifiable information processing and transparency policy and procedures; and c) Review and update the current personally identifiable information processing and transparency: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	The IHGIN IT Security Policy outlines the technical and non-technical controls and requirements for the handling of PII.

Control ID	**PT-2**	Control Name	**Authority to Process Personally Identifiable Information**
Definition	a) Determine and document the [Assignment: organization-defined authority] that permits the [Assignment: organization-defined processing] of personally identifiable information; and b) Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is authorized.		
IHGIN Response	The creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII is conducted by employees duly authorized to conduct said actions. All interactions with PII is audited and monitored in real-time.		

Control ID	**PT-2(1)**	Control Name	**DATA TAGGING**
Definition	Attach data tags containing [Assignment: organization-defined permissible processing] to [Assignment: organization-defined elements of personally identifiable information].		
IHGIN Response	IHGIN tags the specific tables that store PII and use that tagging to implement appropriate privacy controls.		

Control ID	**PT-2(2)**	Control Name	**AUTOMATION**
Definition	Manage enforcement of the authorized processing of personally identifiable information using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	The monitoring and enforcement of controls around the usage of PII is automated through our SIEM solution.		

Control ID	**PT-3**	Control Name	**Personally Identifiable Information Processing Purposes**

Definition	a) Identify and document the [Assignment organization-defined purpose(s)] for processing personally identifiable information; b) Describe the purpose(s) in the public privacy notices and policies of the organization; c) Restrict the [Assignment: organization-defined processing] of personally identifiable information to only that which is compatible with the identified purpose(s); and d) Monitor changes in processing personally identifiable information and implement [Assignment: organization-defined mechanisms] to ensure that any changes are made in accordance with [Assignment: organization-defined requirements].
IHGIN Response	Prior to accepting PII from a customer, the need for that information to be transmitted to IHGIN is analyzed and determined. If determined to meet the needs of the customer, the information being transferred is considered to determine that the least amount of PII is transferred as possible. Any changes to data being sent to IHGIN have to be approved by the customer and these changes are monitored.

Control ID	**PT-3(1)**	Control Name	**DATA TAGGING**
Definition	Attach data tags containing the following purposes to [Assignment: organization-defined elements of personally identifiable information]: [Assignment: organization-defined processing purposes].		
IHGIN Response	Data is tagged and isolated per customer.		

Control ID	**PT-3(2)**	Control Name	**AUTOMATION**
Definition	Track processing purposes of personally identifiable information using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	The monitoring and enforcement of controls around the usage of PII is automated through our SIEM solution.		

Control ID	**PT-4**	Control Name	**Minimization**
Definition	Implement the privacy principle of minimization using [Assignment: organization defined processes].		
IHGIN Response	Prior to accepting PII from a customer, the need for that information to be transmitted to IHGIN is analyzed and determined. If determined to meet the needs of the customer, the information being transferred is considered to determine that the least amount of PII is transferred as possible.		

Control ID	**PT-5**	Control Name	**Consent**
Definition	Implement [Assignment: organization-defined tools or mechanisms] for individuals to consent to the processing of their personally identifiable information prior to its collection that: a) Facilitate individuals' informed decision-making; and b) Provide a means for individuals to decline consent.		

IHGIN Response	IHGIN asks that the customer provide consent to ingest the data being sent to IHGIN systems. Consent can be declined by the customer at any time for any reason.

Control ID	**PT-5(1)**	Control Name	**TAILORED CONSENT**
Definition	Provide [Assignment: organization-defined mechanisms] to allow individuals to tailor processing permissions to selected elements of personally identifiable information.		
IHGIN Response	The customer can tailor the consent for the processing and handling of PII how they wish. IHGIN will comply with these requests.		

Control ID	**PT-5(2)**	Control Name	**JUST-IN-TIME CONSENT**
Definition	Present [Assignment: organization-defined consent mechanisms] to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action.		
IHGIN Response	IHGIN is not collecting information directly from individuals but is instead being handed the information from the customer. It is not possible for IHGIN to ask customers directly for consent at the time of collection.		

Control ID	**PT-6**	Control Name	**Privacy Notice**
Definition	Provide notice to individuals about the processing of personally identifiable information that: a) Is available to individuals upon first interacting with an organization, and subsequently at [Assignment: organization-defined frequency]; b) Is clear and easy-to-understand, expressing information about personally identifiable information processing in plain language; c) Identifies the authority that authorizes the processing of personally identifiable information; d) Identifies the purposes for which personally identifiable information is to be processed; and e) Includes [Assignment: organization-defined information].		
IHGIN Response	IHGIN is not collecting information directly from individuals but is instead being handed the information from the customer. It is not possible to provide a privacy notice directly to individuals at the time of collection.		

Control ID	**PT-6(1)**	Control Name	**JUST-IN-TIME NOTICE**
Definition	Present notice of personally identifiable information processing to individuals at a time and location where the individual provides personally identifiable information or in conjunction with a data action, or [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN is not collecting information directly from individuals but is instead being handed the information from the customer. It is not possible to provide a privacy notice directly to individuals at the time of collection.		

Control ID	**PT-6(2)**	Control Name	**PRIVACY ACT STATEMENTS**

Definition	Include Privacy Act statements on forms that collect information that will be maintained in a Privacy Act system of records, or provide Privacy Act statements on separate forms that can be retained by individuals.
IHGIN Response	IHGIN is not collecting information directly from individuals but is instead being handed the information from the customer. It is not possible to provide a privacy act statements directly to individuals at the time of collection.

Control ID	**PT-7**	Control Name	**System of Records Notice**
Definition	For systems that process information that will be maintained in a Privacy Act system of records: a) Draft system of records notices in accordance with OMB guidance and submit new and significantly modified system of records notices to the OMB and appropriate congressional committees for advance review; b) Publish system of records notices in the Federal Register; and c) Keep system of records notices accurate, up-to-date, and scoped in accordance with policy.		
IHGIN Response	IHGIN is not a federal agency and does not submit records notices under Public Law 93-579 PRIVACT.		

Control ID	**PT-7(1)**	Control Name	**ROUTINE USES**
Definition	Review all routine uses published in the system of records notice at [Assignment: organization-defined frequency] to ensure continued accuracy, and to ensure that routine uses continue to be compatible with the purpose for which the information was collected.		
IHGIN Response	IHGIN is not a federal agency and does not submit records notices under Public Law 93-579 PRIVACT.		

Control ID	**PT-7(2)**	Control Name	**EXEMPTION RULES**
Definition	Review all Privacy Act exemptions claimed for the system of records at [Assignment: organization-defined frequency] to ensure they remain appropriate and necessary in accordance with law, that they have been promulgated as regulations, and that they are accurately described in the system of records notice		
IHGIN Response	IHGIN is not a federal agency and does not submit records notices under Public Law 93-579 PRIVACT.		

Control ID	**PT-8**	Control Name	**Specific Categories of Personally Identifiable Information**
Definition	Apply [Assignment: organization-defined processing conditions] for specific categories of personally identifiable information.		
IHGIN Response	All PII is treated with the same urgency and criticality to ensure that there is no lapse in judgement that could lead to potential disclosure.		

Control ID	**PT-8(1)**	Control Name	**SOCIAL SECURITY NUMBERS**
Definition	When a system processes Social Security numbers:		

	a) Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to their use as a personal identifier; b) Do not deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his or her Social Security number; and c) Inform any individual who is asked to disclose his or her Social Security number whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.
IHGIN Response	IHGIN does not currently collect Social Security Numbers, or foresee the business need to do so under current operations or contracts. If there is a need to collect and use Social Security Numbers, security controls will be put in place to establish clear and defined methodologies of storage and usage.

Control ID	**PT-8(2)**	Control Name	**FIRST AMENDMENT INFORMATION**
Definition	Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual or unless pertinent to and within the scope of an authorized law enforcement activity.		
IHGIN Response	IHGIN is not a federal agency and is not subject under Public Law 93-579 PRIVACT. IHGIN does not force any criteria that could potentially limit first amendment rights on customers.		

Control ID	**PT-9**	Control Name	**Computer Matching Requirements**
Definition	When a system or organization processes information for the purpose of conducting a matching program: a) Obtain approval from the Data Integrity Board to conduct the matching program; b) Develop and enter into a computer matching agreement; c) Publish a matching notice in the Federal Register; d) Independently verify the information produced by the matching program before taking adverse action against an individual, if required; and e) Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.		
IHGIN Response	This is not applicable as IHGIN is not a federal agency, nor is IHGIN utilizing a federal register.		

Risk Assessment

Control ID	**RA-1**	Control Name	**POLICY AND PROCEDURES**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] risk assessment policy that:		

	a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and c) Review and update the current risk assessment: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	IHGIN utilizes a risk management strategy as an integral part of establishing internal policies and procedures. The security and privacy policies are in-part developed as a function of the risk management strategy as a whole.

Control ID	**RA-2**	Control Name	**Security Categorization**
Definition	a) Categorize the system and information it processes, stores, and transmits; b) Document the security categorization results, including supporting rationale, in the security plan for the system; and c) Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.		
IHGIN Response	Systems and data are categorized based upon the environment they will be hosted within. The security categorization depends on the risk associated with the data and overall security of the system. This is analyzed on a per system basis when developing the internal system security plan.		

Control ID	**RA-2(1)**	Control Name	**IMPACT-LEVEL PRIORITIZATION**
Definition	Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.		
IHGIN Response	This is done internally and reviewed periodically to see if prioritization of systems have changed.		

Control ID	**RA-3**	Control Name	**Risk Assessment**
Definition	a) Conduct a risk assessment, including: 1. The likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and 2. The likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information; b) Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;		

	c) Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]]; d) Review risk assessment results [Assignment: organization-defined frequency]; e) Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and f) Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.
IHGIN Response	Internal risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, and other organizations on the operation and use of systems. Risk assessments also consider risk from external parties, including individuals accessing organizational systems; contractors operating systems on behalf of the organization; service providers; and outsourcing entities. Risk assessments are conducted on all 3 levels of the risk management hierarchy. The organization level, business process level, and finally the systems level.

Control ID	**RA-3(1)**	Control Name	**SUPPLY CHAIN RISK ASSESSMENT**
Definition	a) Assess supply chain risks associated with [Assignment: organization-defined systems, system components, and system services]; and b) Update the supply chain risk assessment [Assignment: organization-defined frequency], when there are significant changes to the relevant supply chain, or when changes to the system, environments of operation, or other conditions may necessitate a change in the supply chain.		
IHGIN Response	The potential for supply chain related events is analyzed at the operational level. As a function of the supply chain risk assessment IHGIN utilizes a tool and die shop and actively tests alternate products in order ensure that disruptions to the supply chain can be overcome. Additionally, IHGIN maintains extra materials on-hand and off-site to help overcome any short term disruption that may occur.		

Control ID	**RA-3(2)**	Control Name	**USE OF ALL-SOURCE INTELLIGENCE**
Definition	Use all-source intelligence to assist in the analysis of risk.		
IHGIN Response	IHGIN utilizes an all-source form of intelligence gathering to help inform potential risk.		

Control ID	**RA-3(3)**	Control Name	**DYNAMIC THREAT AWARENESS**
Definition	Determine the current cyber threat environment on an ongoing basis using [Assignment: organization-defined means].		
IHGIN Response	IHGIN IT security personnel practice dynamic threat awareness and may adaptively change controls to a more secure methodology in the case that one becomes available, or the current standard is shown to have a vulnerability.		

Control ID	**RA-3(4)**	Control Name	**PREDICTIVE CYBER ANALYTICS**

Definition	Employ the following advanced automation and analytics capabilities to predict and identify risks to [Assignment: organization-defined systems or system components]: [Assignment: organization-defined advanced automation and analytics capabilities].
IHGIN Response	IHGIN utilizes a predictive cyber analytics engine to analyze incoming traffic and detect both malware and network based intrusion attempts.

Control ID	**RA-4**	Control Name	**Risk Assessment Update**
Definition	Deprecated (Implemented in RA-3)		
IHGIN Response	See response to RA-3		

Control ID	**RA-5**	Control Name	**Vulnerability Monitoring and Scanning**
Definition	a) Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported; b) Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c) Analyze vulnerability scan reports and results from vulnerability monitoring; d) Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; e) Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and f) Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.		
IHGIN Response	IHGIN utilizes an industry leading vulnerability assessment engine that actively scans local systems for potential vulnerabilities and alerts IT to any new vulnerabilities that may be opened by extension of a new known vulnerability or through threat analysis.		

Control ID	**RA-5(1)**	Control Name	**UPDATE TOOL CAPABILITY**
Definition	Deprecated (Implemented in RA-5)		
IHGIN Response	See response to RA-5		

Control ID	**RA-5(2)**	Control Name	**UPDATE SYSTEM VULNERABILITIES**
Definition	Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].		

IHGIN Response	The vulnerability scanner is updated daily and scans are run on some systems on a weekly basis and on critical systems daily.

Control ID	**RA-5(3)**	Control Name	**BREADTH AND DEPTH OF COVERAGE**
Definition	Define the breadth and depth of vulnerability scanning coverage.		
IHGIN Response	The breadth and depth of vulnerability scanning is limited to anything with a network connection and all services.		

Control ID	**RA-5(4)**	Control Name	**DISCOVERABLE INFORMATION**
Definition	Determine information about the system that is discoverable and take [Assignment: organization-defined corrective actions].		
IHGIN Response	The vulnerability scanning solution will highlight any banner or motd information that could lead to information leakage such as versions and service information on systems. Where available, IT will put measures in place to prevent this information from being advertised.		

Control ID	**RA-5(5)**	Control Name	**PRIVILEGED ACCESS**
Definition	Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].		
IHGIN Response	The vulnerability scanning service can utilize the local laps account where necessary to conduct more intrusive scans. This access is audited and if found to be outside of the baseline the SIEM will take immediate action and block the account.		

Control ID	**RA-5(6)**	Control Name	**AUTOMATED TREND ANALYSES**
Definition	Compare the results of multiple vulnerability scans using [Assignment: organization defined automated mechanisms].		
IHGIN Response	The SIEM solution provides automated tend analysis utilizing machine learning to determine if incoming connections potentially may contain a zero-day attack or internal connections are outside of the users established normal behavioral patterns.		

Control ID	**RA-5(7)**	Control Name	**AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS**
Definition	Deprecated (Implemented in CM-8)		
IHGIN Response	See response to CM-8		

Control ID	**RA-5(8)**	Control Name	**REVIEW HISTORIC AUDIT LOGS**
Definition	Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].		
IHGIN Response	Historic audit logs are reviewed during investigations and periodically by IT staff as needed.		

Control ID	**RA-5(9)**	Control Name	**PENETRATION TESTING AND ANALYSES**
Definition	Deprecated (Implemented in CA-8)		
IHGIN Response	See response to CA-8		

Control ID	**RA-5(10)**	Control Name	**CORRELATE SCANNING INFORMATION**
Definition	Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.		
IHGIN Response	The vulnerability assessment engine reports on potential multi-hop attack vectors or multi-vulnerability attacks.		

Control ID	**RA-5(11)**	Control Name	**PUBLIC DISCLOSURE PROGRAM**
Definition	Establish an [Assignment: organization-defined public reporting channel] for receiving reports of vulnerabilities in organizational systems and system components.		
IHGIN Response	IHGIN systems are not publicly accessible.		

Control ID	**RA-6**	Control Name	**Technical Surveillance Countermeasures Survey**
Definition	Employ a technical surveillance countermeasures survey at [Assignment: organization defined locations] [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined events or indicators occur]].		
IHGIN Response	IHGIN is not holding secret government information or data and thus does not currently conduct technical surveillance countermeasures.		

Control ID	**RA-7**	Control Name	**Risk Response**
Definition	Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance.		
IHGIN Response	When a risk is identified, IHGIN IT staff will put a plan in place to mitigate the risk at the earliest possible time.		

Control ID	**RA-8**	Control Name	**Privacy Impact Assessments**
Definition	Conduct privacy impact assessments for systems, programs, or other activities before: a) Developing or procuring information technology that processes personally identifiable information; and b) Initiating a new collection of personally identifiable information that: 1. Will be processed using information technology; and 2. Includes personally identifiable information permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the federal government.		

IHGIN Response	Each system has a privacy impact assessment conducted to ensure that PII is clearly identified.

Control ID	**RA-9**	Control Name	**Criticality Analysis**
Definition	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].		
IHGIN Response	IHGIN has identified critical systems as part of the disaster recovery plan.		

Control ID	**RA-10**	Control Name	**Threat Hunting**
Definition	a) Establish and maintain a cyber threat hunting capability to: 1. Search for indicators of compromise in organizational systems; and 2. Detect, track, and disrupt threats that evade existing controls; and b) Employ the threat hunting capability [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN IT has the internal capability to conduct cyber threat hunting and conduct these exercises as part of investigating potential breaches and SIEM alerts.		

System and Services Acquisition

Control ID	**SA-1**	Control Name	**POLICY AND PROCEDURES**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] system and services acquisition policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and c) Review and update the current system and services acquisition: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency]		
IHGIN Response	IHGIN utilizes risk management procedures along with the security policy and security procedures/plan in order to implement the SA family of controls.		

Control ID	**SA-2**	Control Name	**Allocation of Resources**

Definition	a) Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning; b) Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and c) Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.
IHGIN Response	IHGIN ensures that IT security resources are considered and allocated according to the requirements of the system or system services. A discrete line item does not exist budgetarily but is instead factored into the cost of each project independently to ensure that return on risk is calculated in the most effective manner.

Control ID	**SA-3**	Control Name	**System Development Life Cycle**
Definition	a) Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations; b) Define and document information security and privacy roles and responsibilities throughout the system development life cycle; c) Identify individuals having information security and privacy roles and responsibilities; and d) Integrate the organizational information security and privacy risk management process into system development life cycle activities.		
IHGIN Response	IHGIN ensures that the system development life cycle is designed around ensuring that operations meet ongoing IT Security Policy requirements and are using the security engineering principles highlighted in control SA-8.		

Control ID	**SA-3(1)**	Control Name	**MANAGE PREPRODUCTION ENVIRONMENT**
Definition	Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.		
IHGIN Response	The preproduction or “test” environment as referred to internally is managed to ensure systems match production closely.		

Control ID	**SA-3(2)**	Control Name	**USE OF LIVE OR OPERATIONAL DATA**
Definition	a) Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and b) Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.		
IHGIN Response	IHGIN will scrub data prior to moving it into the preproduction environment to ensure that PII is not contained within the test environment.		

Control ID	**SA-3(3)**	Control Name	**TECHNOLOGY REFRESH**
Definition	Plan for and implement a technology refresh schedule for the system throughout the system development life cycle		

IHGIN Response	IHGIN plans IT systems replacement around a 5-year capital plan and capital lifecycle.

Control ID	**SA-4**	Control Name	**Acquisition Process**
Definition	a) Security and privacy functional requirements; b) Strength of mechanism requirements; c) Security and privacy assurance requirements; d) Controls needed to satisfy the security and privacy requirements; e) Security and privacy documentation requirements; f) Requirements for protecting security and privacy documentation; g) Description of the system development environment and environment in which the system is intended to operate; h) Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and i) Acceptance criteria.		
IHGIN Response	The acquisition process for equipment ensures that security and ongoing support requirements meet the needs of the organizational IT Security Policy.		

Control ID	**SA-4(1)**	Control Name	**FUNCTIONAL PROPERTIES OF CONTROLS**
Definition	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented		
IHGIN Response	IHGIN development team provides a description of the properties of different controls that have been implemented within software.		

Control ID	**SA-4(2)**	Control Name	**DESIGN AND IMPLEMENTATION INFORMATION FOR CONTROLS**
Definition	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].		
IHGIN Response	IHGIN development team provides a description of the properties of different controls that have been implemented within software.		

Control ID	**SA-4(3)**	Control Name	**DEVELOPMENT METHODS, TECHNIQUES, AND PRACTICES**
Definition	Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes: a) [Assignment: organization-defined systems engineering methods]; b) [Assignment: organization-defined [Selection (one or more): systems security; privacy] engineering methods]; c) [Assignment: organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes].		

IHGIN Response	IHGIN development team follows a system development life cycle that includes state-of-the-practice software development methods, systems engineering methods, systems security and privacy engineering methods, and quality control processes helps to reduce the number and severity of the latent errors within systems, system components, and system services.

Control ID	**SA-4(4)**	Control Name	**ASSIGNMENT OF COMPONENTS TO SYSTEMS**
Definition	Deprecated (Implemented in CM-8(9))		
IHGIN Response	See response to CM-8(9)		

Control ID	**SA-4(5)**	Control Name	**SYSTEM, COMPONENT, AND SERVICE CONFIGURATIONS**
Definition	Require the developer of the system, system component, or system service to: a) Deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented; and b) Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.		
IHGIN Response	IHGIN requires the development team to maintain configuration defaults and the configurations are monitored by the SIEM solution to ensure that changes to configuration are approved and implemented by IT staff.		

Control ID	**SA-4(6)**	Control Name	**USE OF INFORMATION ASSURANCE PRODUCTS**
Definition	a) Employ only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and b) Ensure that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.		
IHGIN Response	IT uses NSA approved solutions where applicable and available. Due to being in a manufacturing facility, often industrial control systems will not have passed this level of rigor and require that the IT security of these systems be directly managed.		

Control ID	**SA-4(7)**	Control Name	**NIAP-APPROVED PROTECTION PROFILES**
Definition	a) Limit the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)- approved Protection Profile for a specific technology type, if such a profile exists; and b) Require, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS validated or NSA-approved.		

IHGIN Response	IHGIN requires the use of FIPS validated encryption methodologies within the environment. NAIP-approved protection profiles are implemented where applicable and available. Some industrial control systems do not have the capabilities internally to provide this level of functionality and thus other security controls need to be put in place such as air-gapping network.

Control ID	**SA-4(8)**	Control Name	**CONTINUOUS MONITORING PLAN FOR CONTROLS**
Definition	Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that contains the following level of detail: [Assignment: organization-defined level of detail].		
IHGIN Response	IHGIN continuously monitors the organization and new cyber risks to determine if the level of controls used is appropriate.		

Control ID	**SA-4(9)**	Control Name	**FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES IN USE**
Definition	Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.		
IHGIN Response	Developers internally have to define all functions, ports, protocols, and services in use. IT maintains an ongoing list of systems services, function, ports, and protocols and a per system basis.		

Control ID	**SA-4(10)**	Control Name	**USE OF APPROVED PIV PRODUCTS**
Definition	Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.		
IHGIN Response	IHGIN is not a federal organization and is not subject to this subsection of the PRIVACT.		

Control ID	**SA-4(11)**	Control Name	**SYSTEM OF RECORDS**
Definition	Include [Assignment: organization-defined Privacy Act requirements] in the acquisition contract for the operation of a system of records on behalf of an organization to accomplish an organizational mission or function.		
IHGIN Response	IHGIN is not a federal organization and is not subject to this subsection of the PRIVACT.		

Control ID	**SA-4(12)**	Control Name	**DATA OWNERSHIP**
Definition	a) Include organizational data ownership requirements in the acquisition contract; and b) Require all data to be removed from the contractor's system and returned to the organization within [Assignment: organization-defined timeframe].		
IHGIN Response	IHGIN has established data ownership controls in the IHGIN Security Policy.		

Control ID	**SA-5**	Control Name	**System Documentation**

Definition	a) Obtain administrator documentation for the system, system component, or system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security and privacy functions and mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative or privileged functions; b) Obtain user documentation for the system, system component, or system service that describes: 1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and 3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals; c) Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and takes [Assignment: organization-defined actions] in response; d) Protect documentation as required, in accordance with the organizational risk management strategy; and e) Distribute documentation to [Assignment: organization-defined personnel or roles].
IHGIN Response	IHGIN IT staff maintain this documentation.

Control ID	**SA-6**	Control Name	**Software Usage Restrictions**
Definition	Deprecated (Implemented in CM-10 & SI-7)		
IHGIN Response	See response to SM-10 & SI-7		

Control ID	**SA-7**	Control Name	**User-Installed Software**
Definition	Deprecated (Implemented in CM-11 & SI-7)		
IHGIN Response	See response to CM-11 & SI-7		

Control ID	**SA-8**	Control Name	**Security and Privacy Engineering Principles**
Definition	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].		
IHGIN Response	IHGIN applies systems security and privacy engineering principles to all internal systems ensuring they are maintained throughout the system development life cycle. IHIGN		

	ensures that systems security and privacy engineering principles are applied to new systems, upgraded systems, and legacy systems internally.

Control ID	**SA-8(1)**	Control Name	**CLEAR ABSTRACTIONS**
Definition	Implement the security design principle of clear abstractions.		
IHGIN Response	The principle of clear abstractions is utilized in the systems design process. How the interface functions, and the data inputs and outputs are mapped in clear and simply terms in order to ensure that functional behavior promotes the ease of analysis, inspection, and testing.		

Control ID	**SA-8(2)**	Control Name	**LEAST COMMON MECHANISM**
Definition	Implement the security design principle of least common mechanism in [Assignment: organization-defined systems or system components].		
IHGIN Response	The principle of least common mechanism is followed to reduce the ability of attackers to use remote channels to gain access to systems data.		

Control ID	**SA-8(3)**	Control Name	**MODULARITY AND LAYERING**
Definition	Implement the security design principles of modularity and layering in [Assignment: organization-defined systems or system components].		
IHGIN Response	IHGIN develops in a modular fashion ensuring that the programmed services exist within layers. This allows the organization to change code within one module without impacting functionality within another.		

Control ID	**SA-8(4)**	Control Name	**PARTIALLY ORDERED DEPENDENCIES**
Definition	Implement the security design principle of partially ordered dependencies in [Assignment: organization-defined systems or system components].		
IHGIN Response	IHGIN uses the principle of partially ordered dependencies where available as part of the layering approach to development.		

Control ID	**SA-8(5)**	Control Name	**EFFICIENTLY MEDIATED ACCESS**
Definition	Implement the security design principle of efficiently mediated access in [Assignment: organization-defined systems or system components].		
IHGIN Response	IHGIN utilizes the principle of efficiently mediated access and expressed constraints where available within the hardware configuration.		

Control ID	**SA-8(6)**	Control Name	**MINIMIZED SHARING**
Definition	Implement the security design principle of minimized sharing in [Assignment: organization-defined systems or system components].		
IHGIN Response	IHGIN minimizes the sharing of resources between system components. Processes and functions are to be developed independently of one another where possible.		

Control ID	**SA-8(7)**	Control Name	**REDUCED COMPLEXITY**

Definition	Implement the security design principle of reduced complexity in [Assignment: organization-defined systems or system components].
IHGIN Response	IHGIN aims to ensure that systems and services designed internally provide only the functionality required

Control ID	**SA-8(8)**	Control Name	**SECURE EVOLVABILITY**
Definition	Implement the security design principle of secure evolvability in [Assignment: organization-defined systems or system components].		
IHGIN Response	When systems are evolved to add new or enhanced features the requirements of the feature are defined prior to being put into the product backlog. This ensures that development and systems staff have a clear idea of security requirements so that systems can evolve in a safe and controlled manner.		

Control ID	**SA-8(9)**	Control Name	**TRUSTED COMPONENTS**
Definition	Implement the security design principle of trusted components in [Assignment: organization-defined systems or system components].		
IHGIN Response	IHGIN employs a hierarchical trust relationship of components within the environment.		

Control ID	**SA-8(10)**	Control Name	**HIERARCHICAL TRUST**
Definition	Implement the security design principle of hierarchical trust in [Assignment: organization defined systems or system components].		
IHGIN Response	IHGIN follows the principle of hierarchical trust for components builds on the principle of trusted components and states that the security dependencies in a system will form a partial ordering if they preserve the principle of trusted components.		

Control ID	**SA-8(11)**	Control Name	**INVERSE MODIFICATION THRESHOLD**
Definition	Implement the security design principle of inverse modification threshold in [Assignment: organization-defined systems or system components].		
IHGIN Response	Where applicable IHGIN systems communicate in a 1-way fashion that ensures that modification cannot be conducted through an inverse relationship.		

Control ID	**SA-8(12)**	Control Name	**HIERARCHICAL PROTECTION**
Definition	Implement the security design principle of hierarchical protection in [Assignment: organization-defined systems or system components].		
IHGIN Response	Hierarchical protection is part of the hierarchical trust implementation IHGIN utilizes within system development.		

Control ID	**SA-8(13)**	Control Name	**MINIMIZED SECURITY ELEMENTS**
Definition	Implement the security design principle of minimized security elements in [Assignment: organization-defined systems or system components].		
IHGIN Response	Development and systems staff take extra care when designing systems that only the trusted components needed for the system are trusted.		

Control ID	**SA-8(14)**	Control Name	**LEAST PRIVILEGE**
Definition	Implement the security design principle of least privilege in [Assignment: organization defined systems or system components].		
IHGIN Response	The principle of least privilege is extended into the development and systems design side of IT operations.		

Control ID	**SA-8(15)**	Control Name	**PREDICATE PERMISSION**
Definition	Implement the security design principle of predicate permission in [Assignment: organization-defined systems or system components].		
IHGIN Response	IHGIN development and systems teams coordinate their required permissions and review them internally to provide a review of permissions prior to implementation.		

Control ID	**SA-8(16)**	Control Name	**SELF-RELIANT TRUSTWORTHINESS**
Definition	Implement the security design principle of self-reliant trustworthiness in [Assignment: organization-defined systems or system components].		
IHGIN Response	External systems are not trusted unless the data transferred between the systems is monitored and controlled. Systems are designed to rely only on components internally where available.		

Control ID	**SA-8(17)**	Control Name	**SECURE DISTRIBUTED COMPOSITION**
Definition	Implement the security design principle of secure distributed composition in [Assignment: organization-defined systems or system components].		
IHGIN Response	IHGIN relies on cloud providers to ensure that any distributed system developed internally follows the principle of secure distributed composition.		

Control ID	**SA-8(18)**	Control Name	**TRUSTED COMMUNICATIONS CHANNELS**
Definition	Implement the security design principle of trusted communications channels in [Assignment: organization-defined systems or system components].		
IHGIN Response	Communications channels between systems exist within a trust relationship and are encrypted where required as per the IHGIN IT Security Policy.		

Control ID	**SA-8(19)**	Control Name	**CONTINUOUS PROTECTION**
Definition	Implement the security design principle of continuous protection in [Assignment: organization-defined systems or system components].		
IHGIN Response	Development and systems staff work together to ensure the principle of continuous protection is maintained throughout the development lifecycle.		

Control ID	**SA-8(20)**	Control Name	**SECURE METADATA MANAGEMENT**
Definition	Implement the security design principle of secure metadata management in [Assignment: organization-defined systems or system components].		

IHGIN Response	Metadata is considered a first class object and protection of metadata is outlined within the IHGIN Security Policy.

Control ID	**SA-8(21)**	Control Name	**SELF-ANALYSIS**
Definition	Implement the security design principle of self-analysis in [Assignment: organization defined systems or system components].		
IHGIN Response	Where applicable systems will conduct self-analysis to ensure that systems files remain trusted and unedited by third party interaction. The SIEM solution monitors all system files to ensure that if self-analysis fails that IT can intervene.		

Control ID	**SA-8(22)**	Control Name	**ACCOUNTABILITY AND TRACEABILITY**
Definition	Implement the security design principle of accountability and traceability in [Assignment: organization-defined systems or system components].		
IHGIN Response	All changes to information and actions conducted within IHGIN applications is designed to be audited and provide logs for log collection and analysis.		

Control ID	**SA-8(23)**	Control Name	**SECURE DEFAULTS**
Definition	Implement the security design principle of secure defaults in [Assignment: organization defined systems or system components].		
IHGIN Response	The default configuration for any system deployed is required to follow the IHGIN IT Security Policy.		

Control ID	**SA-8(24)**	Control Name	**SECURE FAILURE AND RECOVERY**
Definition	Implement the security design principle of secure failure and recovery in [Assignment: organization-defined systems or system components].		
IHGIN Response	If a security control within an application or system is detected to have failed, the systems access is disabled by IT as a precautionary step until IT has investigated the issue. For mission critical systems, multiple nodes are configured to ensure that services do not fail during the recovery stage.		

Control ID	**SA-8(25)**	Control Name	**ECONOMIC SECURITY**
Definition	Implement the security design principle of economic security in [Assignment: organization defined systems or system components].		
IHGIN Response	The principle of economic security is a function of internal risk assessments that project the potential cost of exposure and ensure that systems implemented are within that cost or that the risk is disclosed to the client/customer.		

Control ID	**SA-8(26)**	Control Name	**PERFORMANCE SECURITY**
Definition	Implement the security design principle of performance security in [Assignment: organization-defined systems or system components].		
IHGIN Response	IHGIN utilizes a log collect and SIEM solution to conduct internal analysis of traffic offloading this from local systems. Systems are designed to run while utilizing local security controls and encryption methods without degradation.		

Control ID	**SA-8(27)**	Control Name	**HUMAN FACTORED SECURITY**
Definition	Implement the security design principle of human factored security in [Assignment: organization-defined systems or system components]		
IHGIN Response	For internally developed systems the principle of human factored security is implemented. For some of the other IHGIN systems IT is required to make changes not only for security purposes, but also due to the expertise required to operate the system.		

Control ID	**SA-8(28)**	Control Name	**ACCEPTABLE SECURITY**
Definition	Implement the security design principle of acceptable security in [Assignment: organization-defined systems or system components].		
IHGIN Response	The principle of acceptable security is practiced. IHGIN wants customers to feel comfortable with IHGIN data handling procedures and policies and designs systems to meet the expectations of the customer.		

Control ID	**SA-8(29)**	Control Name	**REPEATABLE AND DOCUMENTED PROCEDURES**
Definition	Implement the security design principle of repeatable and documented procedures in [Assignment: organization-defined systems or system components].		
IHGIN Response	Internal security procedures and policies are documented and meant to be repeatable as a function if disaster recovery and succession planning.		

Control ID	**SA-8(30)**	Control Name	**PROCEDURAL RIGOR**
Definition	Implement the security design principle of procedural rigor in [Assignment: organization defined systems or system components].		
IHGIN Response	Procedural rigor is a key component of manufacturing to ensure that defects do not enter the environment. This is practiced throughout the organization.		

Control ID	**SA-8(31)**	Control Name	**SECURE SYSTEM MODIFICATION**
Definition	Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].		
IHGIN Response	Modifications to systems and patch management undergoes testing pre and post implementation along with vulnerability assessments to ensure that systems modifications are not introducing vulnerabilities into the environment.		

Control ID	**SA-8(32)**	Control Name	**SUFFICIENT DOCUMENTATION**
Definition	Implement the security design principle of sufficient documentation in [Assignment: organization-defined systems or system components].		
IHGIN Response	IHGIN IT might be accused of providing excessive documentation on systems security designs and implementation.		

Control ID	**SA-9**	Control Name	**External System Services**

Definition	a) Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls]; b) Define and document organizational oversight and user roles and responsibilities with regard to external system services; and c) Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].
IHGIN Response	Any external system service provided must comply with organization security policy or it will not be allowed to connect to IHGIN systems.

Control ID	**SA-9(1)**	Control Name	**RISK ASSESSMENTS AND ORGANIZATIONAL APPROVALS**
Definition	a) Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and b) Verify that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].		
IHGIN Response	IHGIN conducts organizational risk assessments prior to entering into any partnership or acquisition.		

Control ID	**SA-9(2)**	Control Name	**IDENTIFICATION OF FUNCTIONS, PORTS, PROTOCOLS, AND SERVICES**
Definition	Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services].		
IHGIN Response	External systems access if utilized by a third party require the ports, protocols, and ip addresses of said systems so that IHGIN IT can configure access control lists to limit the access of the connecting system only to the information required.		

Control ID	**SA-9(3)**	Control Name	**ESTABLISH AND MAINTAIN TRUST RELATIONSHIP WITH PROVIDERS**
Definition	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].		
IHGIN Response	IHGIN ensures that trust relationships with third parties are clearly defined and the expectation is mutual that both parties will follow the policies of the other for the connecting systems internally.		

Control ID	**SA-9(4)**	Control Name	**CONSISTENT INTERESTS OF CONSUMERS AND PROVIDERS**
Definition	Take the following actions to verify that the interests of [Assignment: organization defined external service providers] are consistent with and reflect organizational interests: [Assignment: organization-defined actions].		
IHGIN Response	IHGIN takes steps when entering trust relationships that the interests of each party align with the interest of the customers.		

Control ID	**SA-9(5)**	Control Name	**PROCESSING, STORAGE, AND SERVICE LOCATION**
Definition	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].		
IHGIN Response	Trust relationships when established are configured to only have access to the systems and services as agreed upon. The internal SIEM solution monitors all traffic related to the trust relationship and provides IT alerts when the traffic is outside of the control limits of the baselined data.		

Control ID	**SA-9(6)**	Control Name	**ORGANIZATION-CONTROLLED CRYPTOGRAPHIC KEYS**
Definition	Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.		
IHGIN Response	IHGIN maintains exclusive control of cryptographic keys used for encrypted material transmitted through to an external system.		

Control ID	**SA-9(7)**	Control Name	**ORGANIZATION-CONTROLLED INTEGRITY CHECKING**
Definition	Provide the capability to check the integrity of information while it resides in the external system.		
IHGIN Response	IHGIN utilizes checksum data to verify that the information transmitted was received properly.		

Control ID	**SA-9(8)**	Control Name	**PROCESSING AND STORAGE LOCATION — U.S. JURISDICTION**
Definition	Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.		
IHGIN Response	IHGIN always maintains information processing and data storage backup facilities within five eyes nations. Where applicable IHGIN will limit data store to geographic regions and countries in order to comply with security policies and regulations of the jurisdictions served.		

Control ID	**SA-10**	Control Name	**Developer Configuration Management**
Definition	a) Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal]; b) Document, manage, and control the integrity of changes to [Assignment: organization defined configuration items under configuration management]; c) Implement only organization-approved changes to the system, component, or service; d) Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and e) Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].		

IHGIN Response	IHGIN IT enterprise architecture only allows for systems to be update by patches and components provided by the system developer. Any changes to systems is documented, managed, and controlled to ensure the integrity of the data contained and the security posture of the organization is maintained.

Control ID	**SA-10(1)**	Control Name	**SOFTWARE AND FIRMWARE INTEGRITY VERIFICATION**
Definition	Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.		
IHGIN Response	This is a requirement for hardware patches where applicable.		

Control ID	**SA-10(2)**	Control Name	**ALTERNATIVE CONFIGURATION MANAGEMENT PROCESSES**
Definition	Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.		
IHGIN Response	Currently IHGIN does allow members of the IT team to make configuration changes with two sets of eyes on the change and documentation showing the need and outcome of the change as long as the option to roll-back the change exists.		

Control ID	**SA-10(3)**	Control Name	**HARDWARE INTEGRITY VERIFICATION**
Definition	Require the developer of the system, system component, or system service to enable integrity verification of hardware components.		
IHGIN Response	Where available this is implemented.		

Control ID	**SA-10(4)**	Control Name	**TRUSTED GENERATION**
Definition	Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions.		
IHGIN Response	Due to the nature of systems development the option to compare source code and object code is not typically provided by third parties. Instead patch notes are required to be reviewed and maintained as part of the documentation process to review the change if an unintended consequence is detected in testing.		

Control ID	**SA-10(5)**	Control Name	**MAPPING INTEGRITY FOR VERSION CONTROL**
Definition	Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the master build data (hardware drawings and software/firmware code) describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.		
IHGIN Response	This is achieved through the monitoring of patch notes from supported hardware and software vendors.		

Control ID	**SA-10(6)**	Control Name	**TRUSTED DISTRIBUTION**

Definition	Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.
IHGIN Response	A trusted form of distribution including checksum data is required to ensure that patches to hardware, software, and firmware originate from the source.

Control ID	**SA-11**	Control Name	**Developer Testing and Evaluation**
Definition	Require the developer of the system, system component, or system service, at all post design stages of the system development life cycle, to: a) Develop and implement a plan for ongoing security and privacy assessments; b) Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage]; c) Produce evidence of the execution of the assessment plan and the results of the testing and evaluation; d) Implement a verifiable flaw remediation process; and e) Correct flaws identified during testing and evaluation.		
IHGIN Response	Internally this is conducted and achieved through the testing and implementation process conducted prior to release.		

Control ID	**SA-11(1)**	Control Name	**STATIC CODE ANALYSIS**
Definition	Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.		
IHGIN Response	Static code analysis is conducted as part of our internal vulnerability assessment platform. This ensures that outdate libraries or code known to contain vulnerabilities is not implemented into software unwittingly.		

Control ID	**SA-11(2)**	Control Name	**THREAT MODELING AND VULNERABILITY ANALYSES**
Definition	Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that: a) Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels]; b) Employs the following tools and methods: [Assignment: organization-defined tools and methods]; c) Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; and d) Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].		
IHGIN Response	During the development cycle, any changes to planned implementation or requirements is analyzed for risk and any potential threats or vulnerabilities that may		

	be presented are modelled to determine if the change meets internal and external expectation of security.

Control ID	**SA-11(3)**	Control Name	**INDEPENDENT VERIFICATION OF ASSESSMENT PLANS AND EVIDENCE**
Definition	a) Require an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation; and b) Verify that the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information		
IHGIN Response	IHGIN on occasion will have an independent organization assess plans, code, and systems to determine if potential vulnerabilities exist.		

Control ID	**SA-11(4)**	Control Name	**MANUAL CODE REVIEWS**
Definition	Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or techniques].		
IHGIN Response	A manual code review is conducted with two developers working on separate components as part of the code validation process.		

Control ID	**SA-11(5)**	Control Name	**PENETRATION TESTING**
Definition	Require the developer of the system, system component, or system service to perform penetration testing: a) At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; and b) Under the following constraints: [Assignment: organization-defined constraints].		
IHGIN Response	Penetration testing is conducted by the IHGIN IT Security team during regular exercises.		

Control ID	**SA-11(6)**	Control Name	**ATTACK SURFACE REVIEWS**
Definition	Require the developer of the system, system component, or system service to perform attack surface reviews.		
IHGIN Response	Attack surfaces and components are reviewed on a regular basis to ensure that the principle of least requirements is being followed. The vulnerability assessment suite will alert IHGIN IT if a system is responding to protocol requests that are outside of the scope of the system.		

Control ID	**SA-11(7)**	Control Name	**VERIFY SCOPE OF TESTING AND EVALUATION**

Definition	Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigor: [Assignment: organization-defined breadth and depth of testing and evaluation].
IHGIN Response	The scope of testing is defined by both the developer of the system and the IHGIN Enterprise Architect in order to consider both development side and system side tests.

Control ID	**SA-11(8)**	Control Name	**DYNAMIC CODE ANALYSIS**
Definition	Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.		
IHGIN Response	Dynamic code analysis is built into all programs developed by IHGIN.		

Control ID	**SA-11(9)**	Control Name	**INTERACTIVE APPLICATION SECURITY TESTING**
Definition	Require the developer of the system, system component, or system service to employ interactive application security testing tools to identify flaws and document the results.		
IHGIN Response	Instrumentation-based testing is part of the vulnerability testing platform utilized by IHGIN.		

Control ID	**SA-12**	Control Name	**Supply Chain Protection**
Definition	Deprecated (Implemented into the SR Family)		
IHGIN Response	See responses in SR family		

Control ID	**SA-13**	Control Name	**Trustworthiness**
Definition	Deprecated (Implemented in SA-8)		
IHGIN Response	See response to SA-8		

Control ID	**SA-14**	Control Name	**Criticality Analysis**
Definition	Deprecated (Implemented in RA-9)		
IHGIN Response	See response to RA-9		

Control ID	**SA-15**	Control Name	**Development Process, Standards, and Tools**
Definition	a) Require the developer of the system, system component, or system service to follow a documented development process that: 1. Explicitly addresses security and privacy requirements; 2. Identifies the standards and tools used in the development process; 3. Documents the specific tool options and tool configurations used in the development process; and		

	4. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and b) Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements]
IHGIN Response	This control is achieved in the IHGIN Security Policy as the requirements for systems, systems components, and services must comply with the requirements of the Security Policy.

Control ID	**SA-15(1)**	Control Name	**QUALITY METRICS**
Definition	Require the developer of the system, system component, or system service to: a) Define quality metrics at the beginning of the development process; and b) Provide evidence of meeting the quality metrics [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review milestones]; upon delivery]		
IHGIN Response	IHGIN requires all systems developed be delivered with no known vulnerabilities within the CVSS with a severity of medium or high. Any low known vulnerabilities must have vendor provided workarounds applied to ensure operational integrity.		

Control ID	**SA-15(2)**	Control Name	**SECURITY TRACKING TOOLS**
Definition	Require the developer of the system, system component, or system service to select and employ security and privacy tracking tools for use during the development process.		
IHGIN Response	IT utilizes security tracking tools to track security and privacy through the development process.		

Control ID	**SA-15(3)**	Control Name	**CRITICALITY ANALYSIS**
Definition	Require the developer of the system, system component, or system service to perform a criticality analysis: a) At the following decision points in the system development life cycle: [Assignment: organization-defined decision points in the system development life cycle]; and b) At the following level of rigor: [Assignment: organization-defined breadth and depth of criticality analysis].		
IHGIN Response	IHGIN requires a criticality analysis of systems and systems components be conducted as part of the standard operating procedure for the development and implementation of new systems.		

Control ID	**SA-15(4)**	Control Name	**THREAT MODELING AND VULNERABILITY ANALYSIS**
Definition	Deprecated (Implemented in SA-11(2))		
IHGIN Response	See response to SA-11(2)		

Control ID	**SA-15(5)**	Control Name	**ATTACK SURFACE REDUCTION**
Definition	Require the developer of the system, system component, or system service to reduce attack surfaces to [Assignment: organization-defined thresholds].		
IHGIN Response	During the system design process the principle of least functionality is practiced to ensure that the attack surface of any system is reduced to the minimum level possible.		

Control ID	**SA-15(6)**	Control Name	**CONTINUOUS IMPROVEMENT**
Definition	Require the developer of the system, system component, or system service to implement an explicit process to continuously improve the development process.		
IHGIN Response	As a manufacturing company IHGIN is committed to continuous improvement across all operations and organizational levels.		

Control ID	**SA-15(7)**	Control Name	**AUTOMATED VULNERABILITY ANALYSIS**
Definition	Require the developer of the system, system component, or system service [Assignment: organization-defined frequency] to: a) Perform an automated vulnerability analysis using [Assignment: organization-defined tools]; b) Determine the exploitation potential for discovered vulnerabilities; c) Determine potential risk mitigations for delivered vulnerabilities; and d) Deliver the outputs of the tools and results of the analysis to [Assignment: organization-defined personnel or roles].		
IHGIN Response	Internally a vulnerability assessment platform is utilized to conduct vulnerability assessment on devices at regular intervals and report and vulnerabilities found. This is an automated process, but it can be kicked off manually if required by IT. For example after a systems change is implemented a vulnerability scan is conducted to ensure that new vulnerabilities have not been introduced.		

Control ID	**SA-15(8)**	Control Name	**REUSE OF THREAT AND VULNERABILITY INFORMATION**
Definition	Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.		
IHGIN Response	This is a directive internally, and a key function of documentation standards. Previous similar systems or threat assessments can be referenced easily by IT staff as part of day to day operations.		

Control ID	**SA-15(9)**	Control Name	**USE OF LIVE DATA**
Definition	Deprecated (Implemented in SA-3(2))		
IHGIN Response	See response to SA-3(2)		

Control ID	**SA-15(10)**	Control Name	**INCIDENT RESPONSE PLAN**
Definition	Require the developer of the system, system component, or system service to provide, implement, and test an incident response plan.		

IHGIN Response	Anytime a new system is implemented the incident response plan is updated and the new system is tested to ensure that the backup plan and response plan is functional.

Control ID	**SA-15(11)**	Control Name	**ARCHIVE SYSTEM OR COMPONENT**
Definition	Require the developer of the system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security and privacy review.		
IHGIN Response	Documentation is a key part of ensuring that archived systems or component configurations can easily be referenced for the implementation of similar systems or new systems that perform a similar function.		

Control ID	**SA-15(12)**	Control Name	**MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION**
Definition	Require the developer of the system or system component to minimize the use of personally identifiable information in development and test environments.		
IHGIN Response	IHGIN takes steps to ensure that PII is limited on the basis of need and that interactions with PII are minimized to only the interactions required.		

Control ID	**SA-16**	Control Name	**Developer-Provided Training**
Definition	Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [Assignment: organization-defined training].		
IHGIN Response	The developer is required to create training material and train an internal trainer on how to use the program to ensure that the content is delivered to staff in the easiest to digest fashion.		

Control ID	**SA-17**	Control Name	**Developer Security Architecture and Design**
Definition	Require the developer of the system, system component, or system service to produce a design specification and security architecture that: a) Is consistent with the organization's security architecture that is an integral part the organization's enterprise architecture; b) Accurately and completely describes the required security functionality, and the allocation of controls among physical and logical components; and c) Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.		
IHGIN Response	The Enterprise Architect is responsible for reviewing all architecture prior to implementation to ensure that is follows the organizational enterprise architecture plan and the overall security strategy of the organization.		

Control ID	**SA-17(1)**	Control Name	**FORMAL POLICY MODEL**
Definition	Require the developer of the system, system component, or system service to:		

	a) Produce, as an integral part of the development process, a formal policy model describing the [Assignment: organization-defined elements of organizational security policy] to be enforced; and b) Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security policy when implemented.
IHGIN Response	Where available a formal policy model is used in development.

Control ID	**SA-17(2)**	Control Name	**SECURITY-RELEVANT COMPONENTS**
Definition	Require the developer of the system, system component, or system service to: a) Define security-relevant hardware, software, and firmware; and b) Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.		
IHGIN Response	IHGIN maintains an active patch management strategy that requires rationale for any software, hardware, or firmware patch that has not been applied. In the case of the patch providing a solution to a known CVE, the patch is to be applied or additional controls put in place to mitigate the risk.		

Control ID	**SA-17(3)**	Control Name	**FORMAL CORRESPONDENCE**
Definition	Require the developer of the system, system component, or system service to: a) Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects; b) Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model; c) Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; d) Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security relevant hardware, software, and firmware.		
IHGIN Response	IHGIN requires development staff to informally provide this information internally. IT systems staff are to ensure this information is maintained within maintenance window requests and documentation.		

Control ID	**SA-17(4)**	Control Name	**INFORMAL CORRESPONDENCE**
Definition	Require the developer of the system, system component, or system service to: a) Produce, as an integral part of the development process, an informal descriptive top level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;		

	b) Show via [Selection: informal demonstration, convincing argument with formal methods as feasible] that the descriptive top-level specification is consistent with the formal policy model; c) Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware; d) Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and e) Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security relevant hardware, software, and firmware.
IHGIN Response	Development staff provide this information informally during daily stand up meetings and during the code review process. IT systems staff are required to take a formal approach to this methodology.

Control ID	**SA-17(5)**	Control Name	**CONCEPTUALLY SIMPLE DESIGN**
Definition	Require the developer of the system, system component, or system service to: a) Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and b) Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.		
IHGIN Response	IHGIN prefers systems designs and process designs to remain simple in order to limit complexity on operators and potential for errors.		

Control ID	**SA-17(6)**	Control Name	**STRUCTURE FOR TESTING**
Definition	Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate testing.		
IHGIN Response	The developer of the system, system component, or system service is required to structure security-relevant hardware, software, and firmware to facilitate testing.		

Control ID	**SA-17(7)**	Control Name	**STRUCTURE FOR LEAST PRIVILEGE**
Definition	Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.		
IHGIN Response	The principle of least privilege is discussed during the daily stand-up meetings between the developer and the project manager. Additionally, this is reviewed again during code review by a third party to ensure that systems meet the needs of the user.		

Control ID	**SA-17(8)**	Control Name	**ORCHESTRATION**
Definition	Design [Assignment: organization-defined critical systems or system components] with coordinated behavior to implement the following capabilities: [Assignment: organization defined capabilities, by system or component].		

IHGIN Response	Systems architecture is documented to show internal system reliance. For example, systems may be reliant on internal DNS to function. Thus DNS has been configured to be fault tolerant and the reliance documented in the internal system notes.

Control ID	**SA-17(9)**	Control Name	**DESIGN DIVERSITY**
Definition	Use different designs for [Assignment: organization-defined critical systems or system components] to satisfy a common set of requirements or to provide equivalent functionality.		
IHGIN Response	IHGIN utilizes the code review process to provide design diversity.		

Control ID	**SA-18**	Control Name	**Tamper Resistance and Detection**
Definition	Deprecated (Implemented in SR-9)		
IHGIN Response	See response to SR-9		

Control ID	**SA-19**	Control Name	**Component Authenticity**
Definition	Deprecated (Implemented in SR-11)		
IHGIN Response	See response to SR-11		

Control ID	**SA-20**	Control Name	**Customized Development of Critical Components**
Definition	Re-implement or custom develop the following critical system components: [Assignment: organization-defined critical system components].		
IHGIN Response	On the operational security side if a certain system component has a security vulnerability and is no longer supported by the vendor, a customized solution for that critical component is created through a combination of our internal mechanical engineering team and our programming and systems security staff. On the IT side, unsupported hardware is not utilized in the environment. A replacement schedule of items along with end of life is maintained by IT staff to ensure the organization remains within vendor support parameters.		

Control ID	**SA-21**	Control Name	**Developer Screening**
Definition	Require that the developer of [Assignment: organization-defined system, system component, or system service]: a) Has appropriate access authorizations as determined by assigned [Assignment: organization defined official government duties]; b) Satisfies the following additional personnel screening criteria: [Assignment: organization defined additional personnel screening criteria]; and c) Provides information that the access authorizations and screening criteria are satisfied		
IHGIN Response	Developer access is screened and treated the same as all IHGIN users.		

Control ID	**SA-21(1)**	Control Name	**VALIDATION OF SCREENING**
Definition	Deprecated (Implemented in SA-21)		
IHGIN Response	See response to SA-21		

Control ID	**SA-22**	Control Name	**Unsupported System Components**
Definition	a) Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or b) Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].		
IHGIN Response	When components are no longer supported and become legacy systems, they become isolated on the network until a new system component that is supported can be installed or that the system is replaced.		

Control ID	**SA-22(1)**	Control Name	**ALTERNATIVE SOURCES FOR CONTINUED SUPPORT**
Definition	Deprecated (Implemented in SA-22)		
IHGIN Response	See response to SA-22		

Control ID	**SA-23**	Control Name	**Specialization**
Definition	Employ [Selection (one or more): design modification, augmentation, reconfiguration] on [Assignment: organization-defined systems or system components] supporting mission essential services or functions to increase the trustworthiness in those systems or components.		
IHGIN Response	IHGIN has several specialized systems designed internally and the modification, augmentation, and reconfiguration on those systems cannot in any way decrease the trustworthiness of those systems or components.		

System and Communications Protection

Control ID	**SC-1**	Control Name	**POLICY AND PROCEDURES**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] system and communications protection policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and		

	2. Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and c) Review and update the current system and communications protection: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	System and communications protection and requirements are outlined in the IHGIN Security Policy and enforced through technical and procedural controls to ensure compliance.

Control ID	**SC-2**	Control Name	**Separation of System and User Functionality**
Definition	Separate user functionality, including user interface services, from system management functionality.		
IHGIN Response	Systems services and user functionality are maintained independently of one another. Systems management functionality is maintained through accounts that are separate from the daily use accounts of internal IT staff.		

Control ID	**SC-2(1)**	Control Name	**INTERFACES FOR NON-PRIVILEGED USERS**
Definition	Prevent the presentation of system management functionality at interfaces to non-privileged users.		
IHGIN Response	Users are prevented from access information and systems management functionality typical of privileged users.		

Control ID	**SC-2(2)**	Control Name	**DISASSOCIABILITY**
Definition	Store state information from applications and software separately.		
IHGIN Response	This information is collected and stored in an alternate location to ensure disassociability.		

Control ID	**SC-3**	Control Name	**Security Function Isolation**
Definition	Isolate security functions from nonsecurity functions		
IHGIN Response	Security function are isolated from non-security functions using isolation boundaries.		

Control ID	**SC-3(1)**	Control Name	**HARDWARE SEPARATION**
Definition	Employ hardware separation mechanisms to implement security function isolation.		
IHGIN Response	Hardware separation is deployed where available using storage attributes. For example, readable or writeable data.		

Control ID	**SC-3(2)**	Control Name	**ACCESS AND FLOW CONTROL FUNCTIONS**

Definition	Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.
IHGIN Response	Access and flow control is implemented to prevent security functions being conducted by nonsecurity function.

Control ID	**SC-3(3)**	Control Name	**MINIMIZE NONSECURITY FUNCTIONALITY**
Definition	Minimize the number of nonsecurity functions included within the isolation boundary containing security functions.		
IHGIN Response	Systems contained within the isolation boundary are monitored for security relevant events by the internal SIEM solution and the intrusion detection system. The principle of least functionality is in place with these systems to help reduce nonsecurity functions within the isolation boundary.		

Control ID	**SC-3(4)**	Control Name	**MODULE COUPLING AND COHESIVENESS**
Definition	Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.		
IHGIN Response	Inter-module interactions are minimalized as much as possible during the development process to ensure that coupling is minimized.		

Control ID	**SC-3(5)**	Control Name	**LAYERED STRUCTURES**
Definition	Implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.		
IHGIN Response	Inter-layer interactions are minimalized as much as possible during the development process.		

Control ID	**SC-4**	Control Name	**Information in Shared System Resources**
Definition	Prevent unauthorized and unintended information transfer via shared system resources.		
IHGIN Response	Unauthorized or unintended information transfer between shared system resources is picked up by our SIEM solution and internal auditing procedures. Any movement of information that was not intended or is outside of operational norms would be flagged for review by IHGIN IT staff.		

Control ID	**SC-4(1)**	Control Name	**SECURITY LEVELS**
Definition	Deprecated (Implemented in SC-4)		
IHGIN Response	See response to SC-4		

Control ID	**SC-4(2)**	Control Name	**MULTILEVEL OR PERIODS PROCESSING**
Definition	Prevent unauthorized information transfer via shared resources in accordance with [Assignment: organization-defined procedures] when system processing explicitly switches between different information classification levels or security categories.		

IHGIN Response	IHGIN does not current have classified information stored internally. The transfer of information between different levels of system security is prohibited and is automatically flagged by our SIEM solution.

Control ID	**SC-5**	Control Name	**Denial of Service Protection**
Definition	a) [Selection: protect against; limit] the effects of the following types of denial of service events: [Assignment: organization-defined types of denial of service events]; and b) Employ the following controls to achieve the denial of service objective: [Assignment: organization-defined controls by type of denial of service event].		
IHGIN Response	IHGIN maintains denial of service protection through our Internet Service Provided and denial of service detection internally across several different layers of defense.		

Control ID	**SC-5(1)**	Control Name	**RESTRICT ABILITY TO ATTACK OTHER SYSTEMS**
Definition	Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: [Assignment: organization-defined denial of service attacks]		
IHGIN Response	Traffic is analyzed coming in or out of the network and each host based device has it's own IPS installed to detect potential denial of service attacks and block access.		

Control ID	**SC-5(2)**	Control Name	**CAPACITY, BANDWIDTH, AND REDUNDANCY**
Definition	Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial of service attacks.		
IHGIN Response	IHGIN maintains redundant equipment to achieve this goal.		

Control ID	**SC-5(3)**	Control Name	**DETECTION AND MONITORING**
Definition	a) Employ the following monitoring tools to detect indicators of denial of service attacks against, or launched from, the system: [Assignment: organization-defined monitoring tools]; and b) Monitor the following system resources to determine if sufficient resources exist to prevent effective denial of service attacks: [Assignment: organization-defined system resources].		
IHGIN Response	These monitoring controls are in place using the internal SIEM solution and systems reporting.		

Control ID	**SC-6**	Control Name	**Resource Availability**
Definition	Protect the availability of resources by allocating [Assignment: organization-defined resources] by [Selection (one or more); priority; quota; [Assignment: organization-defined controls]].		
IHGIN Response	Systems resources are designed to meet the long-term needs of the organization. At such a time that resources may become constrained, additional resources can be added into the hyperconverged environment seamlessly in order to extend resource availability to all systems at all times.		

Control ID	**SC-7**	Control Name	**Boundary Protection**
Definition	a) Monitor and control communications at the external interfaces to the system and at key internal interfaces within the system; b) Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and c) Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.		
IHGIN Response	IHGIN monitors boundary communications using cloud base machine learning and reporting and an internal SIEM solution to provide a multi-vendor solution. Subnets and physical layer controls are implemented to protect different security zones from cross contamination and information leakage.		

Control ID	**SC-7(1)**	Control Name	**PHYSICALLY SEPARATED SUBNETWORKS**
Definition	Deprecated (Implemented in SC-7)		
IHGIN Response	See response to SC-7		

Control ID	**SC-7(2)**	Control Name	**PUBLIC ACCESS**
Definition	Deprecated (Implemented in SC-7)		
IHGIN Response	See response to SC-7		

Control ID	**SC-7(3)**	Control Name	**ACCESS POINTS**
Definition	Limit the number of external network connections to the system.		
IHGIN Response	The number of external network connections is limited to 1 active connection at any time.		

Control ID	**SC-7(4)**	Control Name	**EXTERNAL TELECOMMUNICATIONS SERVICES**
Definition	a) Implement a managed interface for each external telecommunication service; b) Establish a traffic flow policy for each managed interface; c) Protect the confidentiality and integrity of the information being transmitted across each interface; d) Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need; e) Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need; f) Prevent unauthorized exchange of control plane traffic with external networks; g) Publish information to enable remote networks to detect unauthorized control plane traffic from internal networks; and h) Filter unauthorized control plane traffic from external networks.		

IHGIN Response	The telecommunications external connection is on a managed interface that is monitored and controlled using an advanced security appliance. This appliance monitors incoming traffic for malware and intrusion detection events along with individual user connections to ensure that information coming over the wire is secure. The incoming data is analyzed at the cloud layer as well and all files are executed within a sandbox to determine if any payload is present prior to being handed off internally to the user.

Control ID	**SC-7(5)**	Control Name	**DENY BY DEFAULT — ALLOW BY EXCEPTION**
Definition	Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more); at managed interfaces; for [Assignment: organization-defined systems]].		
IHGIN Response	This is standard within the firewall for all interfaces.		

Control ID	**SC-7(6)**	Control Name	**RESPONSE TO RECOGNIZED FAILURES**
Definition	Deprecated (Implemented in SC-7(18))		
IHGIN Response	See response to SC-7(18)		

Control ID	**SC-7(7)**	Control Name	**PREVENT SPLIT TUNNELING FOR REMOTE DEVICES**
Definition	Prevent a remote device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.		
IHGIN Response	Split-tunneling detection is enabled on the advanced security appliance and connections terminated if a split tunnel is detected.		

Control ID	**SC-7(8)**	Control Name	**ROUTE TRAFFIC TO AUTHENTICATED PROXY SERVERS**
Definition	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.		
IHGIN Response	Traffic is routers through an authenticated proxy server for analysis.		

Control ID	**SC-7(9)**	Control Name	**RESTRICT THREATENING OUTGOING COMMUNICATIONS TRAFFIC**
Definition	a) Detect and deny outgoing communications traffic posing a threat to external systems; and b) Audit the identity of internal users associated with denied communications.		
IHGIN Response	Outgoing traffic is scanned and analyzed the same as incoming traffic to ensure that attacks are not coming into the network, or going out of the network.		

Control ID	**SC-7(10)**	Control Name	**PREVENT EXFILTRATION**

Definition	a) Prevent the exfiltration of information; and b) Conduct exfiltration tests [Assignment: organization-defined frequency].
IHGIN Response	Data exfiltration is controlled through strict access controls, policies, and auditing by our SIEM solution. Data being sent externally is analyzed to ensure that PII and sensitive data is not transferred externally. IT receives notification of any attempt to do this and will need to manually approve the transmittal of said data.

Control ID	**SC-7(11)**	Control Name	**RESTRICT INCOMING COMMUNICATIONS TRAFFIC**
Definition	Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].		
IHGIN Response	Incoming communications traffic to customer facing systems is restricted by IP address using an access control list.		

Control ID	**SC-7(12)**	Control Name	**HOST-BASED PROTECTION**
Definition	Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components].		
IHGIN Response	Each host has host based protection including an antivirus, firewall, and intrusion detection system.		

Control ID	**SC-7(13)**	Control Name	**ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS**
Definition	Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.		
IHGIN Response	Networks are separated and isolated depending upon the network function. IT maintains a subnet for servers and a subnet for user machines. Another example is the production PLC's are on their own network with only specific machines allows to communicate over the wire to that subnet using encrypted channels.		

Control ID	**SC-7(14)**	Control Name	**PROTECT AGAINST UNAUTHORIZED PHYSICAL CONNECTIONS**
Definition	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].		
IHGIN Response	Port security is turned on and network connections not in use are not terminated in the server closet.		

Control ID	**SC-7(15)**	Control Name	**NETWORKED PRIVILEGED ACCESSES**
Definition	Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.		
IHGIN Response	A dedicated managed interface is used for accessing networked devices using a privileged account.		

Control ID	**SC-7(16)**	Control Name	**PREVENT DISCOVERY OF COMPONENTS AND DEVICES**
Definition	Prevent the discovery of specific system components that represent a managed interface.		
IHGIN Response	This is prevented as the managed interface requires physical access and it does not respond to network probes and scans.		

Control ID	**SC-7(17)**	Control Name	**AUTOMATED ENFORCEMENT OF PROTOCOL FORMATS**
Definition	Enforce adherence to protocol formats.		
IHGIN Response	The firewall performs deep packet inspection to ensure adherence to protocol formats and specifications.		

Control ID	**SC-7(18)**	Control Name	**FAIL SECURE**
Definition	Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device		
IHGIN Response	Systems are designed to fail secure, the boundary protection device specifically will block all traffic if it enters a failed stated instead of forwarding all traffic.		

Control ID	**SC-7(19)**	Control Name	**BLOCK COMMUNICATION FROM NON-ORGANIZATIONALLY CONFIGURED HOSTS**
Definition	Block inbound and outbound communications traffic between [Assignment: organization defined communication clients] that are independently configured by end users and external service providers.		
IHGIN Response	Traffic must be explicitly allowed by IT staff. Communication independently configured by end users will be blocked by default.		

Control ID	**SC-7(20)**	Control Name	**DYNAMIC ISOLATION AND SEGREGATION**
Definition	Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components.		
IHGIN Response	IT can dynamically isolate and segregate systems to their own broadcast domains.		

Control ID	**SC-7(21)**	Control Name	**ISOLATION OF SYSTEM COMPONENTS**
Definition	Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].		
IHGIN Response	IHGIN can isolate communication between system components and block access between system components as needed.		

Control ID	**SC-7(22)**	Control Name	**SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS**

Definition	Implement separate network addresses to connect to systems in different security domains.
IHGIN Response	IHGIN uses separate subnets for different security domains.

Control ID	**SC-7(23)**	Control Name	**DISABLE SENDER FEEDBACK ON PROTOCOL VALIDATION FAILURE**
Definition	Disable feedback to senders on protocol format validation failure.		
IHGIN Response	Feedback to senders is not provided in the case of a validation failure where available. When not available, or required feedback is to be nondescript as to not unintentionally leak data.		

Control ID	**SC-7(24)**	Control Name	**PERSONALLY IDENTIFIABLE INFORMATION**
Definition	For systems that process personally identifiable information: a) Apply the following processing rules to data elements of personally identifiable information: [Assignment: organization-defined processing rules]; b) Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system; c) Document each processing exception; and d) Review and remove exceptions that are no longer supported.		
IHGIN Response	IHGIN Security Policy outlines the clear criteria for the handling, auditing, and storage of PII on internal systems.		

Control ID	**SC-7(25)**	Control Name	**UNCLASSIFIED NATIONAL SECURITY CONNECTIONS**
Definition	Prohibit the direct connection of [Assignment: organization-defined unclassified, national security system] to an external network without the use of [Assignment: organization defined boundary protection device].		
IHGIN Response	IHGIN does not maintain national security connections.		

Control ID	**SC-7(26)**	Control Name	**CLASSIFIED NATIONAL SECURITY SYSTEM CONNECTIONS**
Definition	Prohibit the direct connection of a classified, national security system to an external network without the use of [Assignment: organization-defined boundary protection device].		
IHGIN Response	IHGIN does not contain national security system connections.		

Control ID	**SC-7(27)**	Control Name	**UNCLASSIFIED NON-NATIONAL SECURITY SYSTEM CONNECTIONS**
Definition	Prohibit the direct connection of [Assignment: organization-defined unclassified, non-national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].		

IHGIN Response	IHGIN does not contain national security system connections.

Control ID	**SC-7(28)**	Control Name	**CONNECTIONS TO PUBLIC NETWORKS**
Definition	Prohibit the direct connection of [Assignment: organization-defined system] to a public network.		
IHGIN Response	IHGIN prohibits direct connection to unencrypted public networks, and the use of public networks requires the use of an encrypted VPN tunnel to access the internet.		

Control ID	**SC-7(29)**	Control Name	**SEPARATE SUBNETS TO ISOLATE FUNCTIONS**
Definition	Implement [Selection: physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].		
IHGIN Response	IHGIN has implemented separate subnetworks to isolate critical system components.		

Control ID	**SC-8**	Control Name	**Transmission Confidentiality and Integrity**
Definition	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.		
IHGIN Response	Transmission of data between systems must be encrypted as per the requirements outlined in the IHGIN Security Policy.		

Control ID	**SC-8(1)**	Control Name	**CRYPTOGRAPHIC PROTECTION**
Definition	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.		
IHGIN Response	Transmission of data between systems must be encrypted as per the requirements outlined in the IHGIN Security Policy.		

Control ID	**SC-8(2)**	Control Name	**PRE- AND POST-TRANSMISSION HANDLING**
Definition	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.		
IHGIN Response	Data is encrypted at rest as per the requirements outlined in the IHGIN Security Policy.		

Control ID	**SC-8(3)**	Control Name	**CRYPTOGRAPHIC PROTECTION FOR MESSAGE EXTERNALS**
Definition	Implement cryptographic mechanisms to protect message externals unless otherwise protected by [Assignment: organization-defined alternative physical controls].		
IHGIN Response	Header information is transmitted using encrypted methodologies when available and as required.		

Control ID	**SC-8(4)**	Control Name	**CONCEAL OR RANDOMIZE COMMUNICATIONS**

Definition	Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [Assignment: organization-defined alternative physical controls].
IHGIN Response	Communications patterns are baselines and analyzed in real-time to ensure that communications patterns are not outside of the normalized routine for the organization or user. Deep packet inspection is done on all traffic to ensure it doesn't contain malformed data or inappropriate service commands.

Control ID	**SC-8(5)**	Control Name	**PROTECTED DISTRIBUTION SYSTEM**
Definition	Implement [Assignment: organization-defined protected distribution system] to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.		
IHGIN Response	IHGIN does not house secret or top-secret national security data.		

Control ID	**SC-9**	Control Name	**Transmission Confidentiality**
Definition	Deprecated (Implemented in SC-8)		
IHGIN Response	See response to SC-8		

Control ID	**SC-10**	Control Name	**Network Disconnect**
Definition	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time-period] of inactivity.		
IHGIN Response	When network sessions are not terminated at the end of the connection, they are terminated after the timeout limit has been reached.		

Control ID	**SC-11**	Control Name	**Trusted Path**
Definition	a) Provide a [Selection: physically; logically] isolated trusted communications path for communications between the user and the trusted components of the system; and b) Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: [Assignment: organization-defined security functions].		
IHGIN Response	An irrefutable trusted path has been provided between isolated systems and internal users and other isolated systems.		

Control ID	**SC-11(1)**	Control Name	**IRREFUTABLE COMMUNICATIONS PATH**
Definition	a) Provide a trusted communications path that is irrefutably distinguishable from other communications paths; and b) Initiate the trusted communications path for communications between the [Assignment: organization-defined security functions] of the system and the user.		

IHGIN Response	An irrefutable trusted path has been provided between isolated systems and internal users and other isolated systems.

Control ID	**SC-12**	Control Name	**Cryptographic Key Establishment and Management**
Definition	Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].		
IHGIN Response	Cryptographic key requirements for handling and use are housed in the IHGIN Security Policy.		

Control ID	**SC-12(1)**	Control Name	**AVAILABILITY**
Definition	Maintain availability of information in the event of the loss of cryptographic keys by users.		
IHGIN Response	Cryptographic key maintenance is strictly controlled by IT staff under the criteria established in the Information Security Policy.		

Control ID	**SC-12(2)**	Control Name	**SYMMETRIC KEYS**
Definition	Produce, control, and distribute symmetric cryptographic keys using [Selection: NIST FIPS validated; NSA-approved] key management technology and processes.		
IHGIN Response	Symmetric keys are controlled and distributed using FIPS validated methodologies.		

Control ID	**SC-12(3)**	Control Name	**ASYMMETRIC KEYS**
Definition	Produce, control, and distribute asymmetric cryptographic keys using [Selection: NSA approved key management technology and processes; prepositioned keying material; DoD-approved or DoD-issued Medium Assurance PKI certificates; DoD-approved or DoD issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with organization-defined requirements].		
IHGIN Response	The requirements for asymmetric keys is specified in the IHGIN Security Policy and those requirements are based on DOD approved PKI certificates.		

Control ID	**SC-12(4)**	Control Name	**PKI CERTIFICATES**
Definition	Deprecated (Implemented in SC-12(3))		
IHGIN Response	See response to SC-12(3)		

Control ID	**SC-12(5)**	Control Name	**PKI CERTIFICATES / HARDWARE TOKENS**
Definition	Deprecated (Implemented in SC-12(3))		
IHGIN Response	See response to SC-12(3)		

Control ID	**SC-12(6)**	Control Name	**PHYSICAL CONTROL OF KEYS**
Definition	Maintain physical control of cryptographic keys when stored information is encrypted by external service providers.		
IHGIN Response	IHGIN maintains physical control over cryptographic keys to ensure that keys are not subject to unauthorized disclosure or modification.		

Control ID	**SC-13**	Control Name	**Cryptographic Protection**
Definition	a) Determine the [Assignment: organization-defined cryptographic uses]; and b) Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].		
IHGIN Response	IHGIN utilizes FIPS-validated and NSA approved cryptographic methods as per specifications outlined in the IHGIN IT Security Policy.		

Control ID	**SC-14**	Control Name	**Public Access Protections**
Definition	Deprecated (Implemented in AC and SI family)		
IHGIN Response	See responses to AC and SI family		

Control ID	**SC-15**	Control Name	**Collaborative Computing Devices and Applications**
Definition	a) Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b) Provide an explicit indication of use to users physically present at the devices		
IHGIN Response	Collaborative computing devices are required to have a visual que to indicate that they are activated.		

Control ID	**SC-15(1)**	Control Name	**PHYSICAL OR LOGICAL DISCONNECT**
Definition	Provide [Selection (one or more): physical; logical] disconnect of collaborative computing devices in a manner that supports ease of use.		
IHGIN Response	Collaborative computing devices in board rooms can be physically disconnected.		

Control ID	**SC-15(2)**	Control Name	**BLOCKING INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC**
Definition	Deprecated (Implemented in SC-7)		
IHGIN Response	See response to SC-7		

Control ID	**SC-15(3)**	Control Name	**DISABLING AND REMOVAL IN SECURE WORK AREAS**
Definition	Disable or remove collaborative computing devices and applications from [Assignment: organization-defined systems or system components] in [Assignment: organization-defined secure work areas].		

IHGIN Response	IHGIN does not permit staff to use collaborative computing devices within the plant area.

Control ID	**SC-15(4)**	Control Name	**EXPLICITLY INDICATE CURRENT PARTICIPANTS**
Definition	Provide an explicit indication of current participants in [Assignment: organization-defined online meetings and teleconferences].		
IHGIN Response	Meetings indicated explicitly who will be participating in the collaborative computing event.		

Control ID	**SC-16**	Control Name	**Transmission of Security and Privacy Attributes**
Definition	Associate [Assignment: organization-defined security and privacy attributes] with information exchanged between systems and between system components.		
IHGIN Response	Security attributes are implicitly associated with data transferred between organizational systems and system components as a function of cryptography.		

Control ID	**SC-16(1)**	Control Name	**INTEGRITY VERIFICATION**
Definition	Verify the integrity of transmitted security and privacy attributes		
IHGIN Response	Integrity verification checks are conducted to ensure that transmitted data remains in the original state.		

Control ID	**SC-16(2)**	Control Name	**ANTI-SPOOFING MECHANISMS**
Definition	Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process.		
IHGIN Response	Anti-spoofing is achieved by utilizing cryptography in transit.		

Control ID	**SC-17**	Control Name	**Public Key Infrastructure Certificates**
Definition	a) Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and b) Include only approved trust anchors in trust stores or certificate stores managed by the organization.		
IHGIN Response	Public key certificates are obtained from an approved service provider.		

Control ID	**SC-18**	Control Name	**Mobile Code**
Definition	a) Define acceptable and unacceptable mobile code and mobile code technologies; and b) Authorize, monitor, and control the use of mobile code within the system		
IHGIN Response	Mobile code is monitored by the security appliance by using deep packet inspection to determine if there is any malicious code being transmitted between systems.		

Control ID	**SC-18(1)**	Control Name	**IDENTIFY UNACCEPTABLE CODE AND TAKE CORRECTIVE ACTIONS**
Definition	Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].		
IHGIN Response	Unacceptable code is identified using AI and heuristic analysis of data while in transit.		

Control ID	**SC-18(2)**	Control Name	**ACQUISITION, DEVELOPMENT, AND USE**
Definition	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].		
IHGIN Response	IT verified that all programs and systems pass their internal testing procedure to ensure that mobile code deployed meets security requirements.		

Control ID	**SC-18(3)**	Control Name	**PREVENT DOWNLOADING AND EXECUTION**
Definition	Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].		
IHGIN Response	Deep packet inspection and cloud-based execution of code is conducted prior to external code being moved into the IHGIN network. This is done to ensure that unacceptable mobile code does not enter the environment.		

Control ID	**SC-18(4)**	Control Name	**PREVENT AUTOMATIC EXECUTION**
Definition	Prevent the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforce [Assignment: organization-defined actions] prior to executing the code.		
IHGIN Response	Mobile code is prevented from executing automatically. The user or system must take action to execute code.		

Control ID	**SC-18(5)**	Control Name	**ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS**
Definition	Allow execution of permitted mobile code only in confined virtual machine environments.		
IHGIN Response	Mobile code is executed first within a virtual machine that is created in the cloud prior to transmittal into the IHGIN network. This sandboxes the data and executes the code to determine if there is a malicious payload. If deemed to be safe, the code is then transferred internally.		

Control ID	**SC-19**	Control Name	**Voice over Internet Protocol**
Definition	Deprecated (Implemented by other controls for protocols)		
IHGIN Response			

Control ID	**SC-20**	Control Name	**Secure Name/Address Resolution Service (Authoritative Source)**

Definition	a) Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and b) Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.
IHGIN Response	Address resolution must come from an authoritative source. DNSSEC is used internally to ensure child zones and DNS spoofing are prevented.

Control ID	**SC-20(1)**	Control Name	**CHILD SUBSPACES**
Definition	Deprecated (Incorporated in SC-20)		
IHGIN Response	See response to SC-20		

Control ID	**SC-20(2)**	Control Name	**DATA ORIGIN AND INTEGRITY**
Definition	Provide data origin and integrity protection artifacts for internal name/address resolution queries.		
IHGIN Response	DNSSEC is used to achieve this control.		

Control ID	**SC-21**	Control Name	**Secure Name/Address Resolution Service (Recursive or Caching Resolver)**
Definition	Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources		
IHGIN Response	Address resolution must come from an authoritative source. DNSSEC is used internally to ensure child zones and DNS spoofing are prevented.		

Control ID	**SC-21(1)**	Control Name	**DATA ORIGIN AND INTEGRITY**
Definition	Deprecated (Implemented in SC-21)		
IHGIN Response	See response to SC-21		

Control ID	**SC-22**	Control Name	**Architecture and Provisioning for Name/Address Resolution Service**
Definition	Ensure the systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal and external role separation		
IHGIN Response	IHGIN has removed the single point of failure by deploying three authoritative DNS servers through the organization. The DNS servers are geographically redundant.		

Control ID	**SC-23**	Control Name	**Session Authenticity**
Definition	Protect the authenticity of communications sessions.		

IHGIN Response	Sessions are encrypted at the session level in order to transmit the data in a secure fashion.

Control ID	**SC-23(1)**	Control Name	**INVALIDATE SESSION IDENTIFIERS AT LOGOUT**
Definition	Invalidate session identifiers upon user logout or other session termination.		
IHGIN Response	Session identifiers are invalidates upon user logout or after the sessions is terminated.		

Control ID	**SC-23(2)**	Control Name	**USER-INITIATED LOGOUTS AND MESSAGE DISPLAYS**
Definition	Deprecated (Implemented in AC-12(1))		
IHGIN Response	See response to AC-12(1)		

Control ID	**SC-23(3)**	Control Name	**UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS**
Definition	Generate a unique session identifier for each session with [Assignment: organization defined randomness requirements] and recognize only session identifiers that are system generated.		
IHGIN Response	Unique session ids are generated with each session.		

Control ID	**SC-23(4)**	Control Name	**UNIQUE SESSION IDENTIFIERS WITH RANDOMIZATION**
Definition	Deprecated (Implemented in SC-23(3))		
IHGIN Response	See response to SC-23(3)		

Control ID	**SC-23(5)**	Control Name	**ALLOWED CERTIFICATE AUTHORITIES**
Definition	Only allow the use of [Assignment: organization-defined certificate authorities] for verification of the establishment of protected sessions		
IHGIN Response	Only enterprise trusted certifications can be used for the establishment of protected sessions.		

Control ID	**SC-24**	Control Name	**Fail in Known State**
Definition	Fail to a [Assignment: organization-defined known system state] for the following failures on the indicated components while preserving [Assignment: organization-defined system state information] in failure: [Assignment: list of organization-defined types of system failures on organization-defined system components].		
IHGIN Response	Systems are designed to fail safe to a known state.		

Control ID	**SC-25**	Control Name	**Thin Nodes**
Definition	Employ minimal functionality and information storage on the following system components: [Assignment: organization-defined system components].		

IHGIN Response	IHGIN does not utilize thin clients currently. This can be implemented if required by the customer.

Control ID	**SC-26**	Control Name	**Decoys**
Definition	Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.		
IHGIN Response	IHGIN does have a honeypot configured within the network for detecting malicious attacks.		

Control ID	**SC-26(1)**	Control Name	**DETECTION OF MALICIOUS CODE**
Definition	Deprecated (Implemented in SC-35)		
IHGIN Response	See response to SC-35		

Control ID	**SC-27**	Control Name	**Platform-Independent Applications**
Definition	Include within organizational systems, the following platform independent applications: [Assignment: organization-defined platform-independent applications].		
IHGIN Response	IHGIN utilizes platform-independent applications whenever possible.		

Control ID	**SC-28**	Control Name	**Protection of Information at Rest**
Definition	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].		
IHGIN Response	Information at rest is encrypted as per the requirements specified in the IHGIN Security Policy.		

Control ID	**SC-28(1)**	Control Name	**CRYPTOGRAPHIC PROTECTION**
Definition	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].		
IHGIN Response	Information at rest is encrypted as per the requirements specified in the IHGIN Security Policy.		

Control ID	**SC-28(2)**	Control Name	**OFF-LINE STORAGE**
Definition	Remove the following information from online storage and store off-line in a secure location: [Assignment: organization-defined information].		
IHGIN Response	Access to data stored within online systems is audited and analyzed in real-time by our SIEM solution. This ensures that any access to data that is outside of the user norm is flagged for review by IT staff.		

Control ID	**SC-28(3)**	Control Name	**CRYPTOGRAPHIC KEYS**

Definition	Provide protected storage for cryptographic keys [Selection: [Assignment: organization defined safeguards]; hardware-protected key store].
IHGIN Response	A TPM is used to ensure that the key-store is hardware protected.

Control ID	**SC-29**	Control Name	**Heterogeneity**
Definition	Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components].		
IHGIN Response	IHGIN utilizes multiple security and hardware vendors in the environment in order to reduce homogeneity.		

Control ID	**SC-29(1)**	Control Name	**VIRTUALIZATION TECHNIQUES**
Definition	Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN utilizes hyper-converged virtual infrastructure within the environment.		

Control ID	**SC-30**	Control Name	**Concealment and Misdirection**
Definition	Employ the following concealment and misdirection techniques for [Assignment: organization-defined systems] at [Assignment: organization-defined time-periods] to confuse and mislead adversaries: [Assignment: organization-defined concealment and misdirection techniques].		
IHGIN Response	The hyper-converged infrastructure allows for the concealment and misdirection of operating system information.		

Control ID	**SC-30(1)**	Control Name	**VIRTUALIZATION TECHNIQUES**
Definition	Deprecated (Implemented in SC-29(1))		
IHGIN Response	See response to SC-29(1)		

Control ID	**SC-30(2)**	Control Name	**RANDOMNESS**
Definition	Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.		
IHGIN Response	IHGIN does not deploy randomness as a control within the organization. Currently the system is designed to recognize behavioral patterns and detect abnormalities in behavior. Randomness would generate a significant number of false positives and become problematic from a management standpoint. IHGIN relies on the advanced auditing and machine learning to ensure that attacks are detected.		

	Within operations IHGIN does deploy randomness. Shipments arrive at random times, and different staff members will rotate roles and responsibilities to ensure that materials handling and the supply chain is not open to attack.

Control ID	**SC-30(3)**	Control Name	**CHANGE PROCESSING AND STORAGE LOCATIONS**
Definition	Change the location of [Assignment: organization-defined processing and/or storage] [Selection: [Assignment: organization-defined time frequency]; at random time intervals]].		
IHGIN Response	Processing and storage locations change as a function of the hyper-converged virtual infrastructure.		

Control ID	**SC-30(4)**	Control Name	**MISLEADING INFORMATION**
Definition	Employ realistic, but misleading information in [Assignment: organization-defined system components] about its security state or posture.		
IHGIN Response	IHGIN utilizes honeypots to meet the requirements of this control.		

Control ID	**SC-30(5)**	Control Name	**CONCEALMENT OF SYSTEM COMPONENTS**
Definition	Employ the following techniques to hide or conceal [Assignment: organization-defined system components]: [Assignment: organization-defined techniques].		
IHGIN Response	Systems components and information like version numbers are disabled whenever possible to help conceal systems components.		

Control ID	**SC-31**	Control Name	**Covert Channel Analysis**
Definition	a) Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and b) Estimate the maximum bandwidth of those channels		
IHGIN Response	The vulnerability detection suite of tools automatically conducts covert channel analysis.		

Control ID	**SC-31(1)**	Control Name	**TEST COVERT CHANNELS FOR EXPLOITABILITY**
Definition	Test a subset of the identified covert channels to determine the channels that are exploitable.		
IHGIN Response	The vulnerability detection suite of tools automatically conducts covert channel analysis.		

Control ID	**SC-31(2)**	Control Name	**MAXIMUM BANDWIDTH**
Definition	Reduce the maximum bandwidth for identified covert [Selection (one or more); storage; timing] channels to [Assignment: organization-defined values].		
IHGIN Response	On some systems the maximum bandwidth is limited in order to limit connection speed.		

Control ID	**SC-31(3)**	Control Name	**MEASURE BANDWIDTH IN OPERATIONAL ENVIRONMENTS**
Definition	Measure the bandwidth of [Assignment: organization-defined subset of identified covert channels] in the operational environment of the system.		
IHGIN Response	Bandwidth is measured in the operational environment at the switch in order to ensure optimal performance.		

Control ID	**SC-32**	Control Name	**System Partitioning**
Definition	Partition the system into [Assignment: organization-defined system components] residing in separate [Selection: physical; logical] domains or environments based on [Assignment: organization-defined circumstances for physical or logical separation of components].		
IHGIN Response	Systems are physically partitioned and the hyper-converged infrastructure allows systems to be geographically partitioned.		

Control ID	**SC-32(1)**	Control Name	**SEPARATE PHYSICAL DOMAINS FOR PRIVILEGED FUNCTIONS**
Definition	Partition privileged functions into separate physical domains.		
IHGIN Response	Domains are separated physically for privileged functions.		

Control ID	**SC-33**	Control Name	**Transmission Preparation Integrity**
Definition	Deprecated (Implemented in SC-8)		
IHGIN Response	See response to SC-8		

Control ID	**SC-34**	Control Name	**Non-Modifiable Executable Programs**
Definition	For [Assignment: organization-defined system components], load and execute: a) The operating environment from hardware-enforced, read-only media; and b) The following applications from hardware-enforced, read-only media: [Assignment: organization-defined applications].		
IHGIN Response	Executable programs are protected from end-user modification by being set to read-only.		

Control ID	**SC-34(1)**	Control Name	**NO WRITABLE STORAGE**
Definition	Employ [Assignment: organization-defined system components] with no writeable storage that is persistent across component restart or power on/off.		
IHGIN Response	Where appropriate non-writable storage is utilized. This is a function of permissions and is modified based upon user/business need.		

Control ID	**SC-34(2)**	Control Name	**INTEGRITY PROTECTION AND READ-ONLY MEDIA**
Definition	Protect the integrity of information prior to storage on read-only media and control the media after such information has been recorded onto the media.		

IHGIN Response	Technical controls have been put in place using permissions and data verification to ensure that the integrity of data is maintained when being recorded to read-only media.

Control ID	**SC-34(3)**	Control Name	**HARDWARE-BASED PROTECTION**
Definition	a) Employ hardware-based, write-protect for [Assignment: organization-defined system firmware components]; and b) Implement specific procedures for [Assignment: organization-defined authorized individuals] to manually disable hardware write-protect for firmware modifications and re-enable the write-protect prior to returning to operational mode.		
IHGIN Response	Firmware components and other hardware-based protected devices require the write protection be disabled prior to modification and re-enabled after returning to operational mode.		

Control ID	**SC-35**	Control Name	**External Malicious Code Identification**
Definition	Include system components that proactively seek to identify network-based malicious code or malicious websites.		
IHGIN Response	IHGIN deploys several layers of defense against malicious code execution and identification.		

Control ID	**SC-36**	Control Name	**Distributed Processing and Storage**
Definition	Distribute the following processing and storage components across multiple [Selection: physical locations; logical domains]: [Assignment: organization-defined processing and storage components]		
IHGIN Response	The hyper-converged virtual infrastructure allows the organization to achieve this control.		

Control ID	**SC-36(1)**	Control Name	**POLLING TECHNIQUES**
Definition	a) Employ polling techniques to identify potential faults, errors, or compromises to the following processing and storage components: [Assignment: organization-defined distributed processing and storage components]; and b) Take the following actions in response to identified faults, errors, or compromises: [Assignment: organization-defined actions].		
IHGIN Response	The hyper-converged virtual infrastructure uses polling techniques to identify potential faults or compromises to the processing, storage, and network components.		

Control ID	**SC-36(2)**	Control Name	**SYNCHRONIZATION**
Definition	Synchronize the following duplicate systems or system components: [Assignment: organization-defined duplicate systems or system components].		
IHGIN Response	This is achieved using the hyper-converged virtual infrastructure.		

Control ID	**SC-37**	Control Name	**Out-of-Band Channels**

Definition	Employ the following out-of-band channels for the physical delivery or electronic transmission of [Assignment: organization-defined information, system components, or devices] to [Assignment: organization-defined individuals or systems]: [Assignment: organization-defined out-of-band channels].
IHGIN Response	The transmission of cryptographic key management information is exchanged using out of band channels.

Control ID	**SC-37(1)**	Control Name	**ENSURE DELIVERY AND TRANSMISSION**
Definition	Employ [Assignment: organization-defined controls] to ensure that only [Assignment: organization-defined individuals or systems] receive the following information, system components, or devices: [Assignment: organization-defined information, system components, or devices].		
IHGIN Response	In the case of the exchange of cryptographic key management information, proof of individual identity is required to ensure delivery and transmission.		

Control ID	**SC-38**	Control Name	**Operations Security**
Definition	Employ the following operations security controls to protect key organizational information throughout the system development life cycle: [Assignment: organization-defined operations security controls].		
IHGIN Response	OPSEC controls are applied on the production side of operations to ensure that machine components used in manufacturing are isolated to their own network clear of interference from other networked traffic.		

Control ID	**SC-39**	Control Name	**Process Isolation**
Definition	Maintain a separate execution domain for each executing system process.		
IHGIN Response	Sandboxing is utilized where available to perform process isolation.		

Control ID	**SC-39(1)**	Control Name	**HARDWARE SEPARATION**
Definition	Implement hardware separation mechanisms to facilitate process isolation.		
IHGIN Response	Hardware based memory management is part of the hyper-converged virtual infrastructure.		

Control ID	**SC-39(2)**	Control Name	**SEPARATE EXECUTION DOMAIN PER THREAD**
Definition	Maintain a separate execution domain for each thread in [Assignment: organization defined multi-threaded processing].		
IHGIN Response	Where available this is implemented through sandboxing.		

Control ID	**SC-40**	Control Name	**Wireless Link Protection**
Definition	Protect external and internal [Assignment: organization-defined wireless links] from the following signal parameter attacks: [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].		

IHGIN Response	Wireless link protection is enabled internally through a combination of encryption, radio power management, and hardware-based controls.

Control ID	**SC-40(1)**	Control Name	**ELECTROMAGNETIC INTERFERENCE**
Definition	Implement cryptographic mechanisms that achieve [Assignment: organization-defined level of protection] against the effects of intentional electromagnetic interference.		
IHGIN Response	Cryptographic methods as outlined in the IHGIN Security Policy are a requirement for all wireless connections and help to protect against electromagnetic interference.		

Control ID	**SC-40(2)**	Control Name	**REDUCE DETECTION POTENTIAL**
Definition	Implement cryptographic mechanisms to reduce the detection potential of wireless links to [Assignment: organization-defined level of reduction].		
IHGIN Response	Cryptographic methods as outlined in the IHGIN Security Policy are a requirement for all wireless connections and help to reduce detection potential.		

Control ID	**SC-40(3)**	Control Name	**IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION**
Definition	Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.		
IHGIN Response	Cryptographic methods as outlined in the IHGIN Security Policy are a requirement for all wireless connections and will prevent manipulative communications deception based on signal parameters.		

Control ID	**SC-40(4)**	Control Name	**SIGNAL PARAMETER IDENTIFICATION**
Definition	Implement cryptographic mechanisms to prevent the identification of [Assignment: organization-defined wireless transmitters] by using the transmitter signal parameters		
IHGIN Response	Anti-fingerprinting is enabled on the wireless network.		

Control ID	**SC-41**	Control Name	**Port and I/O Device Access**
Definition	[Selection: Physically or Logically] disable or remove [Assignment: organization-defined connection ports or input/output devices] on the following systems or system components: [Assignment: organization-defined systems or system components].		
IHGIN Response	Input/output devices such as CD, DVD, USB drives, etc have been disabled on local machines as part of the IHGIN Security Policy.		

Control ID	**SC-42**	Control Name	**Sensor Capability and Data**
Definition	a) Prohibit the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions: [Assignment: organization defined exceptions where remote activation of sensors is allowed]; and		

	b) Provide an explicit indication of sensor use to [Assignment: organization-defined class of users].
IHGIN Response	Environmental sensing devices and other sensors are disabled by our mobile device management policy.

Control ID	**SC-42(1)**	Control Name	**REPORTING TO AUTHORIZED INDIVIDUALS OR ROLES**
Definition	Verify that the system is configured so that data or information collected by the [Assignment: organization-defined sensors] is only reported to authorized individuals or roles.		
IHGIN Response	To use environmental sensors on mobile devices administrator level privileges are required to apply the special mobile device management policy to the device.		

Control ID	**SC-42(2)**	Control Name	**AUTHORIZED USE**
Definition	Employ the following measures so that data or information collected by [Assignment: organization-defined sensors] is only used for authorized purposes: [Assignment: organization-defined measures].		
IHGIN Response	To use environmental sensors on mobile devices administrator level privileges are required to apply the special mobile device management policy to the device. This is controlled by IT and requires authorization.		

Control ID	**SC-42(3)**	Control Name	**PROHIBIT USE OF DEVICES**
Definition	Prohibit the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems].		
IHGIN Response	The use of mobile devices is prohibited in certain areas of the facility.		

Control ID	**SC-42(4)**	Control Name	**NOTICE OF COLLECTION**
Definition	Employ the following measures to facilitate an individual's awareness that personally identifiable information is being collected by [Assignment: organization-defined sensors]: [Assignment: organization-defined measures].		
IHGIN Response	Users are notified as part of the onboarding process that data is collected at various points in the organization and that all interactions with network based devices is monitors and logged.		

Control ID	**SC-42(5)**	Control Name	**COLLECTION MINIMIZATION**
Definition	Employ [Assignment: organization-defined sensors] that are configured to minimize the collection of information about individuals that is not needed.		
IHGIN Response	Information collected is limited to the information that IT requires to ensure operational security.		

Control ID	**SC-43**	Control Name	**Usage Restrictions**

Definition	a) Establish usage restrictions and implementation guidelines for the following system components: [Assignment: organization-defined system components]; and b) Authorize, monitor, and control the use of such components within the system.
IHGIN Response	Usage restrictions apply to all systems components and are monitored and analyzed in the SIEM solution.

Control ID	**SC-44**	Control Name	**Detonation Chambers**
Definition	Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location].		
IHGIN Response	Detonation chambers are utilized by the firewall along with deep packet inspection to check incoming files for potentially malicious code.		

Control ID	**SC-45**	Control Name	**System Time Synchronization**
Definition	Synchronize system clocks within and between systems and system components		
IHGIN Response	Time clocks are synchronized using NTP.		

Control ID	**SC-46**	Control Name	**Cross Domain Policy Enforcement**
Definition	Implement a policy enforcement mechanism [Selection: physically; logically] between the physical and/or network interfaces for the connecting security domains.		
IHGIN Response	Cross domain policy enforcement is done using a combination of firewall, IDS, IPS, and SIEM solutions.		

Control ID	**SC-47**	Control Name	**Communications Path Diversity**
Definition	Establish [Assignment: organization-defined alternate communications paths] for system operations organizational command and control.		
IHGIN Response	Alternate communications paths have been implemented in order to protect against a single point of failure.		

Control ID	**SC-48**	Control Name	**Sensor Relocation**
Definition	Relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].		
IHGIN Response	If a deployed IoT device within the network has a known vulnerability that is not patched the device is removed from service until a patch is released.		

Control ID	**SC-48(1)**	Control Name	**DYNAMIC RELOCATION OF SENSORS OR MONITORING CAPABILITIES**
Definition	Dynamically relocate [Assignment: organization-defined sensors and monitoring capabilities] to [Assignment: organization-defined locations] under the following conditions or circumstances: [Assignment: organization-defined conditions or circumstances].		

IHGIN Response	Relocation and disabling of sensors and monitoring equipment is not able to be dynamically relocated due to the nature of a manufacturing environment.

Control ID	**SC-49**	Control Name	**Hardware-Enforced Separation and Policy Enforcement**
Definition	Implement hardware-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].		
IHGIN Response	Hardware enforced separation and policy enforcement is enabled where available.		

Control ID	**SC-50**	Control Name	**Software-Enforced Separation and Policy Enforcement**
Definition	Implement software-enforced separation and policy enforcement mechanisms between [Assignment: organization-defined security domains].		
IHGIN Response	Where hardware enforces separation and policy enforcement is not available, a software based solution is used.		

Control ID	**SC-51**	Control Name	**Operational and Internet-Based Technologies**
Definition	a) Implement the following controls on [Assignment: organization-defined Operational Technology (OT), Internet of Things (IoT), and/or Industrial Internet of Things (IIoT) systems, components, or devices] prior to connecting to [Assignment: organization-defined systems or networks]: [Assignment: organization-defined controls]; or b) Isolate the OT, IoT, and IIoT systems, components, or devices from the designated organizational systems or prohibit network connectivity by the systems, components, or devices.		
IHGIN Response	OT systems like PLC's, SCADA systems, etc that are utilized within our manufacturing environment are separated from our normal operations network. Communications to this network is strictly prohibited and controlled to ensure that OT devices are not subject to data streams that could compromise systems integrity.		

System and Information Integrity

Control ID	**SI-1**	Control Name	**Policy and Procedures**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] system and information integrity policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;		

	b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and c) Review and update the current system and information integrity: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].
IHGIN Response	System and information integrity are achieved through the policies and procedures utilized by IHGIN IT. The IHGIN Security Policy is an integral document that helps to ensure that this family of controls is implemented successfully.

Control ID	**SI-2**	Control Name	**Flaw Remediation**
Definition	a) Identify, report, and correct system flaws; b) Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c) Install security-relevant software and firmware updates within [Assignment: organization defined time-period] of the release of the updates; and d) Incorporate flaw remediation into the organizational configuration management process.		
IHGIN Response	Flaw remediation is part of the continuous improvement program undertaken by IT. Patch management, and vulnerability assessments allow IT to take remediation action to correct organizational security flaws as they are recognized.		

Control ID	**SI-2(1)**	Control Name	**CENTRAL MANAGEMENT**
Definition	Centrally manage the flaw remediation process.		
IHGIN Response	The flaw remediation process is centrally managed by IHGIN IT staff.		

Control ID	**SI-2(2)**	Control Name	**AUTOMATED FLAW REMEDIATION STATUS**
Definition	Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN vulnerability scanner detects firmware versions and software versions and verifies that they are utilizing the most secure version.		

Control ID	**SI-2(3)**	Control Name	**TIME TO REMEDIATE FLAWS AND BENCHMARKS FOR CORRECTIVE ACTIONS**
Definition	a) Measure the time between flaw identification and flaw remediation; and b) Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].		
IHGIN Response	The time between flaw identification and flaw remediation is monitored using the internal IHGIN task system.		

Control ID	**SI-2(4)**	Control Name	**AUTOMATED PATCH MANAGEMENT TOOLS**

Definition	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].
IHGIN Response	IHGIN utilizes WSUS and other automated software patch management tools to ensure that some patches are automatically applied.

Control ID	**SI-2(5)**	Control Name	**AUTOMATIC SOFTWARE AND FIRMWARE UPDATES**
Definition	Install [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined system components].		
IHGIN Response	IHGIN utilizes WSUS and other automated software patch management tools to ensure that some patches are automatically applied.		

Control ID	**SI-2(6)**	Control Name	**REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE AND FIRMWARE**
Definition	Remove previous versions of [Assignment: organization-defined software and firmware components] after updated versions have been installed.		
IHGIN Response	In some cases, rollbacks of approves updates may need to take place. When this happens, it is conducted by It manually.		

Control ID	**SI-3**	Control Name	**Malicious Code Protection**
Definition	a) Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code; b) Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; c) Configure malicious code protection mechanisms to: 1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization defined personnel or roles] in response to malicious code detection. d) Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.		
IHGIN Response	IHGIN conducts malicious code scans at several different layers under the defense in depth methodology. These systems are automatically updated several times daily to ensure that the most recent malicious code signatures have been downloaded and are being used. In the case that a false positive is detected it is investigated with the vendor.		

Control ID	**SI-3(1)**	Control Name	**CENTRAL MANAGEMENT**

Definition	Centrally manage malicious code protection mechanisms
IHGIN Response	The SIEM solution acts as a central management location to report on and inform of malicious code execution attempts.

Control ID	**SI-3(2)**	Control Name	**AUTOMATIC UPDATES**
Definition	Deprecated (Implemented in SI-3)		
IHGIN Response	See response to SI-3		

Control ID	**SI-3(3)**	Control Name	**NON-PRIVILEGED USERS**
Definition	Deprecated (Implemented in AC-6(10))		
IHGIN Response	See response to AC-6(10)		

Control ID	**SI-3(4)**	Control Name	**UPDATES ONLY BY PRIVILEGED USERS**
Definition	Update malicious code protection mechanisms only when directed by a privileged user.		
IHGIN Response	Malicious code protection systems require privileged access to manually update or change configuration.		

Control ID	**SI-3(5)**	Control Name	**PORTABLE STORAGE DEVICES**
Definition	Deprecated (Implemented in MP-7)		
IHGIN Response	See response to MP-7		

Control ID	**SI-3(6)**	Control Name	**TESTING AND VERIFICATION**
Definition	a) Test malicious code protection mechanisms [Assignment: organization-defined frequency] by introducing known benign code into the system; and b) Verify that the detection of the code and the associated incident reporting occur.		
IHGIN Response	Malicious code protection is tested by IT during red team exercises.		

Control ID	**SI-3(7)**	Control Name	**NONSIGNATURE-BASED DETECTION**
Definition	Deprecated (Implemented in SI-3)		
IHGIN Response	See response to SI-3		

Control ID	**SI-3(8)**	Control Name	**DETECT UNAUTHORIZED COMMANDS**
Definition	a) Detect the following unauthorized operating system commands through the kernel application programming interface on [Assignment: organization-defined system hardware components]: [Assignment: organization-defined unauthorized operating system commands]; and		

	b) [Selection (one or more): issue a warning; audit the command execution; prevent the execution of the command].
IHGIN Response	Unauthorized commands for kernel functions are detected by the host based IDS and reported to the SIEM solution in real-time.

Control ID	**SI-3(9)**	Control Name	**AUTHENTICATE REMOTE COMMANDS**
Definition	Implement [Assignment: organization-defined mechanisms] to authenticate [Assignment: organization-defined remote commands].		
IHGIN Response	Remote commands require authentication in order to execute.		

Control ID	**SI-3(10)**	Control Name	**MALICIOUS CODE ANALYSIS**
Definition	a) Employ the following tools and techniques to analyze the characteristics and behavior of malicious code: [Assignment: organization-defined tools and techniques]; and b) Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.		
IHGIN Response	Malicious code analysis is conducted at several different layers within the IHGIN network and systems. The analysis will alert within the SIEM if malicious code is detected and a remediation process/investigation is triggered by IT.		

Control ID	**SI-4**	Control Name	**System Monitoring**
Definition	a) Monitor the system to detect: 1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and 2. Unauthorized local, network, and remote connections; b) Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods]; c) Invoke internal monitoring capabilities or deploy monitoring devices: 1. Strategically within the system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; d) Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; e) Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation; f) Obtain legal opinion regarding system monitoring activities; and g) Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].		
IHGIN Response	IHGIN IT monitors all systems and audit logs using an internal SIEM solution.		

Control ID	**SI-4(1)**	Control Name	**SYSTEM-WIDE INTRUSION DETECTION SYSTEM**
Definition	Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.		
IHGIN Response	The SIEM solution ties together the different levels IDS protection into a system-wide solution.		

Control ID	**SI-4(2)**	Control Name	**AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS**
Definition	Employ automated tools and mechanisms to support near real-time analysis of events		
IHGIN Response	The SIEM solution provided real-time analysis and automated tools and mechanisms that can be triggered by events.		

Control ID	**SI-4(3)**	Control Name	**AUTOMATED TOOL AND MECHANISM INTEGRATION**
Definition	Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms		
IHGIN Response	The SIEM solution provided real-time analysis and automated tools and mechanisms that can be triggered by events.		

Control ID	**SI-4(4)**	Control Name	**INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC**
Definition	Monitor inbound and outbound communications traffic [Assignment: organization-defined [frequency] for unusual or unauthorized activities or conditions.		
IHGIN Response	Inbound and outbound communications traffic is monitored.		

Control ID	**SI-4(5)**	Control Name	**SYSTEM-GENERATED ALERTS**
Definition	Alert [Assignment: organization-defined personnel or roles] when the following system generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].		
IHGIN Response	System generated alerts trigger an investigation/response from IT.		

Control ID	**SI-4(6)**	Control Name	**RESTRICT NON-PRIVILEGED USERS**
Definition	Deprecated (Implemented in AC-6(10))		
IHGIN Response	See response to AC-6(10)		

Control ID	**SI-4(7)**	Control Name	**AUTOMATED RESPONSE TO SUSPICIOUS EVENTS**
Definition	a) Notify [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events; and b) Take the following actions upon detection: [Assignment: organization-defined least disruptive actions to terminate suspicious events].		

IHGIN Response	IHGIN SIEM solution and IDS systems will take automated response to suspicious events.

Control ID	**SI-4(8)**	Control Name	**PROTECTION OF MONITORING INFORMATION**
Definition	Deprecated (Implemented in SI-4)		
IHGIN Response	See response to SI-4		

Control ID	**SI-4(9)**	Control Name	**TESTING OF MONITORING TOOLS AND MECHANISMS**
Definition	Test intrusion-monitoring tools and mechanisms [Assignment: organization-defined frequency].		
IHGIN Response	Monitoring tools and mechanisms are tested frequently during red team exercises.		

Control ID	**SI-4(10)**	Control Name	**VISIBILITY OF ENCRYPTED COMMUNICATIONS**
Definition	Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms].		
IHGIN Response	Encrypted web traffic is monitored using the internal proxy server that uses SSL striping to analyze traffic.		

Control ID	**SI-4(11)**	Control Name	**ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES**
Definition	Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies		
IHGIN Response	The SIEM solution and the Security Appliance look for potential traffic anomalies and will alert to such anomalies and even trigger internal automated actions/alerts to safeguard the network.		

Control ID	**SI-4(12)**	Control Name	**AUTOMATED ORGANIZATION-GENERATED ALERTS**
Definition	Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].		
IHGIN Response	The SIEM solution and the Security Appliance look for potential traffic anomalies and will alert to such anomalies and even trigger internal automated actions/alerts to safeguard the network.		

Control ID	**SI-4(13)**	Control Name	**ANALYZE TRAFFIC AND EVENT PATTERNS**
Definition	a) Analyze communications traffic and event patterns for the system; b) Develop profiles representing common traffic and event patterns; and c) Use the traffic and event profiles in tuning system-monitoring devices.		

IHGIN Response	The SIEM solution analyses traffic and event pattern and utilizes machine learning to monitor this information of traffic and events that are outside of organizational or user norms.

Control ID	**SI-4(14)**	Control Name	**WIRELESS INTRUSION DETECTION**
Definition	Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.		
IHGIN Response	The Wireless network utilizes an IDS.		

Control ID	**SI-4(15)**	Control Name	**WIRELESS TO WIRELINE COMMUNICATIONS**
Definition	Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.		
IHGIN Response	Wireless to wireline communications require deep packet inspection and IDS/IPS be utilized to analyze the traffic.		

Control ID	**SI-4(16)**	Control Name	**CORRELATE MONITORING INFORMATION**
Definition	Correlate information from monitoring tools and mechanisms employed throughout the system.		
IHGIN Response	Monitoring information is correlated using the SIEM solution		

Control ID	**SI-4(17)**	Control Name	**INTEGRATED SITUATIONAL AWARENESS**
Definition	Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.		
IHGIN Response	Monitoring of technological assets is conducted using the SIEM solution, but everyone in the organization is encouraged to bring up potential issues and concerns and abnormal system interaction to IT in order to achieve organization-wide situational awareness.		

Control ID	**SI-4(18)**	Control Name	**ANALYZE TRAFFIC AND COVERT EXFILTRATION**
Definition	Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system].		
IHGIN Response	Oubound traffic conducts deep packet inspection and verifies that data is not being exfiltrated.		

Control ID	**SI-4(19)**	Control Name	**RISK FOR INDIVIDUALS**
Definition	Implement [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.		
IHGIN Response	IT and HR work closely to monitor staffing changes and issues in order to maintain a secure posture and identify potential increased levels of risk among employees.		

Control ID	**SI-4(20)**	Control Name	**PRIVILEGED USERS**
Definition	Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring].		
IHGIN Response	Privileges users are actively monitored and reported on.		

Control ID	**SI-4(21)**	Control Name	**PROBATIONARY PERIODS**
Definition	Implement the following additional monitoring of individuals during [Assignment: organization-defined probationary period]: [Assignment: organization-defined additional monitoring].		
IHGIN Response	Staff within probationary periods monitored to ensure that they are not conducting malicious activity.		

Control ID	**SI-4(22)**	Control Name	**UNAUTHORIZED NETWORK SERVICES**
Definition	a) Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]; and b) [Selection (one or more): audit; alert [Assignment: organization-defined personnel or roles]] when detected.		
IHGIN Response	Unauthorized network services are detected and blocked by the security appliance and SIEM solution.		

Control ID	**SI-4(23)**	Control Name	**HOST-BASED DEVICES**
Definition	Implement the following host-based monitoring mechanisms at [Assignment: organization-defined system components]: [Assignment: organization-defined host-based monitoring mechanisms].		
IHGIN Response	Host-based monitoring is enabled and enforced through group policy.		

Control ID	**SI-4(24)**	Control Name	**INDICATORS OF COMPROMISE**
Definition	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].		
IHGIN Response	Indicators of compromise are reported on via the SIEM solution.		

Control ID	**SI-4(25)**	Control Name	**OPTIMIZE NETWORK TRAFFIC ANALYSIS**
Definition	Provide visibility into network traffic at external and key internal system boundaries to optimize the effectiveness of monitoring devices.		
IHGIN Response	Network traffic is analyzed and subnetworks created in order to optimize network traffic.		

Control ID	**SI-5**	Control Name	**Security Alerts, Advisories, and Directives**
Definition	a) Receive system security alerts, advisories, and directives from [Assignment: organization defined external organizations] on an ongoing basis; b) Generate internal security alerts, advisories, and directives as deemed necessary; c) Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and d) Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.		
IHGIN Response	IHGIN IT receives security alerts, advisories, and directives from security vendors and third-party organizations.		

Control ID	**SI-5(1)**	Control Name	**AUTOMATED ALERTS AND ADVISORIES**
Definition	Broadcast security alert and advisory information throughout the organization using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	Alerting and advising is automated through the SIEM solution and other security platforms utilized by IHGIN IT.		

Control ID	**SI-6**	Control Name	**Security and Privacy Function Verification**
Definition	a) Verify the correct operation of [Assignment: organization-defined security and privacy functions]; b) Perform the verification of the functions specified in SI-6a [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]]; c) Notify [Assignment: organization-defined personnel or roles] of failed security and privacy verification tests; and d) [Selection (one or more): Shut the system down; Restart the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.		
IHGIN Response	Privacy function verification is assured through the Enterprise Architect and tested internally at regular intervals to ensure that systems and privacy attributes are being applied as intended.		

Control ID	**SI-6(1)**	Control Name	**NOTIFICATION OF FAILED SECURITY TESTS**
Definition	Deprecated (Implemented in SI-6)		
IHGIN Response	See response to SI-6		

Control ID	**SI-6(2)**	Control Name	**AUTOMATION SUPPORT FOR DISTRIBUTED TESTING**
Definition	Implement automated mechanisms to support the management of distributed security and privacy function testing		

IHGIN Response	Automated mechanisms are integrated to support the management of the distributed security environment.

Control ID	**SI-6(3)**	Control Name	**REPORT VERIFICATION RESULTS**
Definition	Report the results of security and privacy function verification to [Assignment: organization-defined personnel or roles].		
IHGIN Response	Verification results are reported to the Vice President on a regular basis as part of the IT reporting structure.		

Control ID	**SI-7**	Control Name	**Software, Firmware, and Information Integrity**
Definition	a) Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and b) Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].		
IHGIN Response	Integrity verification tools are used to detect unauthorized changes to software, firmware, and information. When detected the files or system are isolated and an investigation is undertaken by IT.		

Control ID	**SI-7(1)**	Control Name	**INTEGRITY CHECKS**
Definition	Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].		
IHGIN Response	Integrity checks are performed at regular intervals and at startup for IHGIN systems.		

Control ID	**SI-7(2)**	Control Name	**AUTOMATED NOTIFICATIONS OF INTEGRITY VIOLATIONS**
Definition	Employ automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.		
IHGIN Response	Any integrity violation will kickoff an alert for IT to investigate.		

Control ID	**SI-7(3)**	Control Name	**CENTRALLY MANAGED INTEGRITY TOOLS**
Definition	Employ centrally managed integrity verification tools.		
IHGIN Response	Integrity tools are centrally managed.		

Control ID	**SI-7(4)**	Control Name	**TAMPER-EVIDENT PACKAGING**
Definition	Deprecated (Implemented in SR-9)		
IHGIN Response	See response to SR-9		

Control ID	**SI-7(5)**	Control Name	**AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS**
Definition	Automatically [Selection (one or more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered.		
IHGIN Response	Integrity violations will result in a fail-secure state for the system where network access is disabled until IT can resolve the issue.		

Control ID	**SI-7(6)**	Control Name	**CRYPTOGRAPHIC PROTECTION**
Definition	Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.		
IHGIN Response	Software is encrypted at rest. Firmware is encrypted where available.		

Control ID	**SI-7(7)**	Control Name	**INTEGRATION OF DETECTION AND RESPONSE**
Definition	Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].		
IHGIN Response	The SIEM solution will detect and provide IT with notifications to respond to security and systems events.		

Control ID	**SI-7(8)**	Control Name	**AUDITING CAPABILITY FOR SIGNIFICANT EVENTS**
Definition	Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: [Selection (one or more): generate an audit record; alert current user; alert [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined other actions]].		
IHGIN Response	The audit logs are stored separate from the SIEM solution. This allows for manual auditing of records if required outside of the SIEM solution.		

Control ID	**SI-7(9)**	Control Name	**VERIFY BOOT PROCESS**
Definition	Verify the integrity of the boot process of the following system components: [Assignment: organization-defined system components].		
IHGIN Response	The boot process is verified on each machine prior to operation.		

Control ID	**SI-7(10)**	Control Name	**PROTECTION OF BOOT FIRMWARE**
Definition	Implement the following mechanisms to protect the integrity of boot firmware in [Assignment: organization-defined system components]: [Assignment: organization defined mechanisms].		
IHGIN Response	The boot firmware is protected from update and requires bios administrator access to update.		

Control ID	**SI-7(11)**	Control Name	**CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES**
Definition	Deprecated (Implemented in CM-7(6))		
IHGIN Response	See response to CM-7(6)		

Control ID	**SI-7(12)**	Control Name	**INTEGRITY VERIFICATION**
Definition	Require that the integrity of the following user-installed software be verified prior to execution: [Assignment: organization-defined user-installed software].		
IHGIN Response	Users are prohibited from installing software. IHGIN IT administrator will install integrity verified software.		

Control ID	**SI-7(13)**	Control Name	**CODE EXECUTION IN PROTECTED ENVIRONMENTS**
Definition	Deprecated (Implemented in CM-7(7))		
IHGIN Response	See response to CM-7(7)		

Control ID	**SI-7(14)**	Control Name	**BINARY OR MACHINE EXECUTABLE CODE**
Definition	Deprecated (Implemented in CM-7(8))		
IHGIN Response	See response to CM-7(8)		

Control ID	**SI-7(15)**	Control Name	**CODE AUTHENTICATION**
Definition	Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components].		
IHGIN Response	Cryptographic requirements outlined in the IHGIN Security Policy are utilized for code authentication purposes.		

Control ID	**SI-7(16)**	Control Name	**TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION**
Definition	Prohibit processes from executing without supervision for more than [Assignment: organization-defined time-period].		
IHGIN Response	Currently the default timers within the OS are used to control this. These can be changed if required by the customer.		

Control ID	**SI-7(17)**	Control Name	**RUNTIME APPLICATION SELF-PROTECTION**
Definition	Implement [Assignment: organization-defined controls] for application self-protection at runtime.		
IHGIN Response	Runtime application protection is conducted by the local hostbased ids/ips system and reported to the SIEM solution.		

Control ID	**SI-8**	Control Name	**Spam Protection**

Definition	a) Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and b) Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
IHGIN Response	Spam protection is enabled by our cloud-based email provider.

Control ID	**SI-8(1)**	Control Name	**CENTRAL MANAGEMENT**
Definition	Centrally manage spam protection mechanisms.		
IHGIN Response	Spam protection mechanisms are centrally managed.		

Control ID	**SI-8(2)**	Control Name	**AUTOMATIC UPDATES**
Definition	Automatically update spam protection mechanisms [Assignment: organization-defined frequency].		
IHGIN Response	Spam protection policies and databases are automatically updated.		

Control ID	**SI-8(3)**	Control Name	**CONTINUOUS LEARNING CAPABILITY**
Definition	Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.		
IHGIN Response	The spam protection utilizes continuous machine learning to adapt to organizational needs and block spam.		

Control ID	**SI-9**	Control Name	**Information Input Restrictions**
Definition	Deprecated (Implemented in AC Family)		
IHGIN Response	See response to AC family		

Control ID	**SI-10**	Control Name	**Information Input Validation**
Definition	Check the validity of the following information inputs: [Assignment: organization defined information inputs to the system].		
IHGIN Response	Input form validation is conducted as a check across all IHGIN developed systems.		

Control ID	**SI-10(1)**	Control Name	**MANUAL OVERRIDE CAPABILITY**
Definition	a) Provide a manual override capability for input validation of the following information inputs: [Assignment: organization-defined inputs]; b) Restrict the use of the manual override capability to only [Assignment: organization defined authorized individuals]; and c) Audit the use of the manual override capability.		

IHGIN Response	Manual override of form input validation is achieved through TSQL. TSQL commands executed are audited and logged to each user conducting them. As process, TSQL commands require approval prior to operational use.

Control ID	**SI-10(2)**	Control Name	**REVIEW AND RESOLVE OF ERRORS**
Definition	Review and resolve input validation errors within [Assignment: organization-defined time period].		
IHGIN Response	Input validation errors can be reported through customer service and they will be reviewed for resolution in the next software release.		

Control ID	**SI-10(3)**	Control Name	**PREDICTABLE BEHAVIOR**
Definition	Verify that the system behaves in a predictable and documented manner when invalid inputs are received.		
IHGIN Response	The system is verified to function as documented and in a predictable fashion.		

Control ID	**SI-10(4)**	Control Name	**TIMING INTERACTIONS**
Definition	Account for timing interactions among system components in determining appropriate responses for invalid inputs.		
IHGIN Response	TTL and timeout values are set to ensure that responses for inputs are conducted within acceptable timeframes.		

Control ID	**SI-10(5)**	Control Name	**RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS**
Definition	Restrict the use of information inputs to [Assignment: organization-defined trusted sources] and/or [Assignment: organization-defined formats].		
IHGIN Response	Inputs are restricted to trusted sources only and controlled through access control lists.		

Control ID	**SI-10(6)**	Control Name	**INJECTION PREVENTION**
Definition	Prevent untrusted data injections.		
IHGIN Response	SQL injection prevention such as input validation and stored procedures are utilized to prevent untrusted data injections.		

Control ID	**SI-11**	Control Name	**Error Handling**
Definition	a) Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and b) Reveal error messages only to [Assignment: organization-defined personnel or roles].		
IHGIN Response	IHGIN systems generate error messages that provide information required to make corrective action without revealing information that could be exploited.		

Control ID	**SI-12**	Control Name	**Information Management and Retention**
Definition	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.		
IHGIN Response	IHGIN ensures that backup and record retention follow all applicable laws, executive orders, directives, regulations, standards, guidelines, and operational requirements.		

Control ID	**SI-12(1)**	Control Name	**LIMIT PERSONALLY IDENTIFIABLE INFORMATION ELEMENTS**
Definition	Limit personally identifiable information being processed in the information life cycle to the following elements of PII: [Assignment: organization-defined elements of personally identifiable information].		
IHGIN Response	PII is limited only to the information required by the system.		

Control ID	**SI-12(2)**	Control Name	**MINIMIZE PERSONALLY IDENTIFIABLE INFORMATION IN TESTING, TRAINING, AND RESEARCH**
Definition	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].		
IHGIN Response	PII is not used in research, testing, or training. This information is scrubbed prior to being used for these use cases.		

Control ID	**SI-12(3)**	Control Name	**INFORMATION DISPOSAL**
Definition	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].		
IHGIN Response	Disposal and destruction of data after the retention period is conducted by IHGIN as per the guidelines in the Data Destruction Policy.		

Control ID	**SI-13**	Control Name	**Predictable Failure Prevention**
Definition	a) Determine mean time to failure (MTTF) for the following system components in specific environments of operation: [Assignment: organization-defined system components]; and b) Provide substitute system components and a means to exchange active and standby components in accordance with the following criteria: [Assignment: organization-defined MTTF substitution criteria].		
IHGIN Response	Systems are replaced prior to the MTTF as indicated by the vendor.		

Control ID	**SI-13(1)**	Control Name	**TRANSFERRING COMPONENT RESPONSIBILITIES**
Definition	Take system components out of service by transferring component responsibilities to substitute components no later than [Assignment: organization-defined fraction or percentage] of mean time to failure.		

IHGIN Response	Often systems component responsibilities and services are moved to an alternate machine before the MTTF has been reached. On occasion the service may be deprecated and no longer offered.

Control ID	**SI-13(2)**	Control Name	**TIME LIMIT ON PROCESS EXECUTION WITHOUT SUPERVISION**
Definition	Deprecated (Implemented in SI-7(16))		
IHGIN Response	See response to SI-7(16)		

Control ID	**SI-13(3)**	Control Name	**MANUAL TRANSFER BETWEEN COMPONENTS**
Definition	Manually initiate transfers between active and standby system components when the use of the active component reaches [Assignment: organization-defined percentage] of the mean time to failure.		
IHGIN Response	Transfer between systems when MTTF is reached is manually conducted.		

Control ID	**SI-13(4)**	Control Name	**STANDBY COMPONENT INSTALLATION AND NOTIFICATION**
Definition	If system component failures are detected: a) Ensure that the standby components are successfully and transparently installed within [Assignment: organization-defined time-period]; and b) [Selection (one or more): Activate [Assignment: organization-defined alarm]; Automatically shut down the system; [Assignment: organization-defined action]].		
IHGIN Response	If a system component failure is detected the standby component or system takes over as the primary and the failed component is fixed.		

Control ID	**SI-13(5)**	Control Name	**FAILOVER CAPABILITY**
Definition	Provide [Selection: real-time; near real-time] [Assignment: organization-defined failover capability] for the system.		
IHGIN Response	IHGIN has real-time failover capacity in the server environment on-site and near real-time failover capability built into the cloud using the hyper-converged virtual infrastructure.		

Control ID	**SI-14**	Control Name	**Non-Persistence**
Definition	Implement non-persistent [Assignment: organization-defined system components and services] that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at [Assignment: organization-defined frequency]].		
IHGIN Response	Non-persistence is initiated through the firewall to ensure that APT's cannot maintain a persistent state over a long period of time.		

Control ID	**SI-14(1)**	Control Name	**REFRESH FROM TRUSTED SOURCES**
Definition	Obtain software and data employed during system component and service refreshes from the following trusted sources: [Assignment: organization-defined trusted sources].		
IHGIN Response	Trusted sources for vendor hardware and software is outlined in the system documentation.		

Control ID	**SI-14(2)**	Control Name	**NON-PERSISTENT INFORMATION**
Definition	a) [Selection: refresh [Assignment: organization-defined information] [Assignment: organization-defined frequency]; generate [Assignment: organization-defined information] on demand]; and b) Delete information when no longer needed.		
IHGIN Response	Information is not retained for longer than contractually or legally required.		

Control ID	**SI-14(3)**	Control Name	**NON-PERSISTENT CONNECTIVITY**
Definition	Establish connections to the system on demand and terminate connections after [Selection: completion of a request; a period of non-use].		
IHGIN Response	Non-persistence is initiated through the firewall to ensure that APT's cannot maintain a persistent state over a long period of time.		

Control ID	**SI-15**	Control Name	**Information Output Filtering**
Definition	Validate information output from the following software programs and/or applications to ensure that the information is consistent with the expected content: [Assignment: organization-defined software programs and/or applications].		
IHGIN Response	Information output is filtered to ensure that SQL injections cannot product output results that are inconsistent with the output results expected from the software or application.		

Control ID	**SI-16**	Control Name	**Memory Protection**
Definition	Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].		
IHGIN Response	Stack canaries are utilized to help protect memory from buffer over-flow attacks.		

Control ID	**SI-17**	Control Name	**Fail-Safe Procedures**
Definition	Implement the indicated fail-safe procedures when the indicated failures occur: [Assignment: organization-defined list of failure conditions and associated fail-safe procedures].		
IHGIN Response	Systems are designed to fail-secure and fail-safe.		

Control ID	**SI-18**	Control Name	**Personally Identifiable Information Quality Operations**

Definition	a) Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle [Assignment: organization-defined frequency]; and b) Correct or delete inaccurate or outdated personally identifiable information
IHGIN Response	PII is not verified in this way directly, the hashed values are compared to ensure that they match.

Control ID	**SI-18(1)**	Control Name	**AUTOMATION**
Definition	Correct or delete personally identifiable information that is inaccurate or outdated, incorrectly determined regarding impact, or incorrectly de-identified using [Assignment: organization-defined automated mechanisms].		
IHGIN Response	PII is automatically deleted after use in the system.		

Control ID	**SI-18(2)**	Control Name	**DATA TAGS**
Definition	Employ data tags to automate the correction or deletion of personally identifiable information across the information life cycle within organizational systems.		
IHGIN Response	Data tags are used to flag PII through the information life cycle.		

Control ID	**SI-18(3)**	Control Name	**COLLECTION**
Definition	Collect personally identifiable information directly from the individual.		
IHGIN Response	PII is collected from the customer, not directly from the individual.		

Control ID	**SI-18(4)**	Control Name	**INDIVIDUAL REQUESTS**
Definition	Correct or delete personally identifiable information upon request by individuals or their designated representatives.		
IHGIN Response	Information can be manually deleted if requested by the customer.		

Control ID	**SI-18(5)**	Control Name	**NOTICE OF COLLECTION OR DELETION**
Definition	Notify [Assignment: organization-defined recipients of personally identifiable information] and individuals that the personally identifiable information has been corrected or deleted.		
IHGIN Response	A notification will be provided if PII is deleted.		

Control ID	**SI-19**	Control Name	**De-Identification**
Definition	a) Remove the following elements of personally identifiable information from datasets: [Assignment: organization-defined elements of personally identifiable information]; and		

	b) Evaluate [Assignment: organization-defined frequency] for effectiveness of de-identification.
IHGIN Response	Only information required is supplied, nothing more. Deidentification only takes place when creating test data sets for use in the test environment.

Control ID	**SI-19(1)**	Control Name	**COLLECTION**
Definition	De-identify the dataset upon collection by not collecting personally identifiable information.		
IHGIN Response	Deidentification only takes place when creating test data sets for use in the test environment.		

Control ID	**SI-19(2)**	Control Name	**ARCHIVING**
Definition	Prohibit archiving of personally identifiable information elements if those elements in a dataset will not be needed after the dataset is archived.		
IHGIN Response	Only the encrypted PII is archived and is not human readable. The encryption methodologies are outlined in the IHGIN Information Security Policy.		

Control ID	**SI-19(3)**	Control Name	**RELEASE**
Definition	Remove personally identifiable information elements from a dataset prior to its release if those elements in the dataset do not need to be part of the data release.		
IHGIN Response	PII is encrypted and removed after use. It is not stored.		

Control ID	**SI-19(4)**	Control Name	**REMOVAL, MASKING, ENCRYPTION, HASHING, OR REPLACEMENT OF DIRECT IDENTIFIERS**
Definition	Remove, mask, encrypt, hash, or replace direct identifiers in a dataset.		
IHGIN Response	Encryption of the storage media and hashing of the data occurs to help protect PII within the dataset.		

Control ID	**SI-19(5)**	Control Name	**STATISTICAL DISCLOSURE CONTROL**
Definition	Manipulate numerical data, contingency tables, and statistical findings so that no person or organization is identifiable in the results of the analysis.		
IHGIN Response	This can be implemented if required, at this time the reporting mechanism is limited on a per customer basis and no external customer has access to statistics that would possible identify another customer.		

Control ID	**SI-19(6)**	Control Name	**DIFFERENTIAL PRIVACY**
Definition	Prevent disclosure of personally identifiable information by adding non-deterministic noise to the results of mathematical operations before the results are reported.		
IHGIN Response	Non-deterministic salts are applied to the hashing mechanism used to encrypt PII.		

Control ID	**SI-19(7)**	Control Name	**VALIDATED SOFTWARE**
Definition	Perform de-identification using validated algorithms and software that is validated to implement the algorithms.		
IHGIN Response	De-identification software is not utilized at this time.		

Control ID	**SI-19(8)**	Control Name	**MOTIVATED INTRUDER**
Definition	Perform a motivated intruder test on the de-identified dataset to determine if the identified data remains or if the de-identified data can be re-identified.		
IHGIN Response	Red team exercises are conducted on a regular basis as a function of IT operations.		

Control ID	**SI-20**	Control Name	**Tainting**
Definition	Embed data or capabilities in the following systems or system components to determine if organizational data has been exfiltrated or improperly removed from the organization: [Assignment: organization-defined systems or system components].		
IHGIN Response	IHGIN does not employ tainting at this time as the information contained within the database is scrubbed of PII after use.		

Control ID	**SI-21**	Control Name	**Information Refresh**
Definition	Refresh [Assignment: organization-defined information] at [Assignment: organization defined frequencies] or generate the information on demand and delete the information when no longer needed.		
IHGIN Response	IHGIN does not house classified information currently.		

Control ID	**SI-22**	Control Name	**Information Diversity**
Definition	a) Identify the following alternative sources of information for [Assignment: organization defined essential functions and services]: [Assignment: organization-defined alternative information sources]; and b) Use an alternative information source for the execution of essential functions or services on [Assignment: organization-defined systems or system components] when the primary source of information is corrupted or unavailable		
IHGIN Response	Information diversity is limited to only what the customer is required to provide us in order to complete the job.		

Control ID	**SI-23**	Control Name	**Information Fragmentation**
Definition	a) Fragment the following information: [Assignment: organization-defined information]; and b) Distribute the fragmented information across the following systems or system components: [Assignment organization-defined systems or system components].		

IHGIN Response	Information is fragmented through the storage function of the hyper-converged virtualized infrastructure.

Supply Chain Risk Management

Control ID	**SR-1**	Control Name	**Policy and Procedures**
Definition	a) Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): organization-level; mission/business process-level; system level] supply chain risk management policy that: a. Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the supply chain risk management policy and the associated supply chain risk management controls; b) Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the supply chain risk management policy and procedures; and c) Review and update the current supply chain risk management: 1. Policy [Assignment: organization-defined frequency]; and 2. Procedures [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN manages supply chain risk through several internal policies, procedures, and supplier/vendor contractual obligations.		

Control ID	**SR-2**	Control Name	**Supply Chain Risk Management Plan**
Definition	a) Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations, and disposal of the following systems, system components or system services: [Assignment: organization-defined systems, system components, or system services]; b) Implement the supply chain risk management plan consistently across the organization; and c) Review and update the supply chain risk management plan [Assignment: organization defined frequency] or as required, to address threat, organizational or environmental changes.		
IHGIN Response	IHGIN disaster recovery plan considers supply chains risks and the associated changes the organization would need to take if one of the risks was to become a reality.		

Control ID	**SR-2(1)**	Control Name	**ESTABLISH SCRM TEAM**
Definition	Establish a supply chain risk management team consisting of [Assignment: organization defined personnel, roles, and responsibilities] to lead and support the following SCRM activities: [Assignment: organization-defined supply chain risk management activities].		

IHGIN Response	The SCRM team consist of the Director of Operations, VP of Finance, and President of the organization.

Control ID	**SR-3**	Control Name	**Supply Chain Controls and Processes**
Definition	a) Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel]; b) Employ the following supply chain controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls]; and c) Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan; [Assignment: organization defined document]].		
IHGIN Response	The supply chain is continuously monitored to identify potential weaknesses of areas of improvement to better serve customers and keep costs low. Supply chain processes and controls are documented internally.		

Control ID	**SR-3(1)**	Control Name	**DIVERSE SUPPLY BASE**
Definition	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].		
IHGIN Response	IHGIN has a main supplier for each material along with several backup suppliers in the case that the main supplier runs into operational issues.		

Control ID	**SR-3(2)**	Control Name	**LIMITATION OF HARM**
Definition	Employ the following supply chain controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: [Assignment: organization defined controls].		
IHGIN Response	IHGIN reduces harm within the supply chain and systems through ensuring that pre-agreed maintenance schedules are adhered to by certified professionals. Backup systems and materials are maintained on-site and off-site in order to facilitate any backlogs that may occur due to an unforeseen circumstance.		

Control ID	**SR-4**	Control Name	**Provenance**
Definition	Document, monitor, and maintain valid provenance of the following systems, system components, and associated data: [Assignment: organization-defined systems, system components, and associated data].		
IHGIN Response	The chain of custody and maintenance on each pieces of machinery and system is maintained internally.		

Control ID	**SR-4(1)**	Control Name	**IDENTITY**

Definition	Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components: [Assignment: organization-defined supply chain elements, processes, and personnel associated with organization-defined systems and critical system components].
IHGIN Response	IHGIN utilizes ERP software to maintain visibility across the supply chain. Internally a maintenance management solution has been deployed to track all maintenance activities and expenditures on internal production equipment.

Control ID	**SR-4(2)**	Control Name	**TRACK AND TRACE**
Definition	Establish and maintain unique identification of the following systems and critical system components for tracking through the supply chain: [Assignment: organization-defined systems and critical system components].		
IHGIN Response	Unique identification exists for all systems, components, and materials and is fully tracked through the supply chain,		

Control ID	**SR-4(3)**	Control Name	**VALIDATE AS GENUINE AND NOT ALTERED**
Definition	Employ the following controls to validate that the system or system component received is genuine and has not been altered: [Assignment: organization-defined controls].		
IHGIN Response	Materials are validated as genuine as part of the process for the receipt of goods.		

Control ID	**SR-5**	Control Name	**Acquisition Strategies, Tools, and Methods**
Definition	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].		
IHGIN Response	IHGIN requires that materials and equipment arrive with tamper-evident packaging.		

Control ID	**SR-5(1)**	Control Name	**ADEQUATE SUPPLY**
Definition	Employ the following controls to ensure an adequate supply of [Assignment: organization defined critical system components]: [Assignment: organization-defined controls].		
IHGIN Response	IHGIN maintains an inventory of materials and replacement parts and equipment to assure that adequate supply is maintained in the case of a supply chain disruption.		

Control ID	**SR-5(2)**	Control Name	**ASSESSMENTS PRIOR TO SELECTION, ACCEPTANCE, MODIFICATION, OR UPDATE**
Definition	Assess the system, system component, or system service prior to selection, acceptance, modification, or update.		

IHGIN Response	Internal analysis of components, systems, and materials is conducted by the IHGIN engineering team prior to the selection, acceptance, modification, or update of the system.

Control ID	**SR-6**	Control Name	**Supplier Reviews**
Definition	Review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].		
IHGIN Response	IHGIN reviews the performance of all suppliers to ensure that materials and equipment meet the rigorous standards required for a manufacturing facility.		

Control ID	**SR-6(1)**	Control Name	**PENETRATION TESTING AND ANALYSIS**
Definition	Employ [Selection (one or more): organizational analysis, independent third-party analysis, organizational penetration testing, independent third-party penetration testing] of the following supply chain elements, processes, and actors associated with the system, system component, or system service: [Assignment: organization-defined supply chain elements, processes, and actors].		
IHGIN Response	Penetration testing of the manufacturing supply chain is not conducted at this time due to agreements in place. Suppliers are required to have a security policy in place and actively maintain their own security and systems. The operational supply chain is tested during penetration tests.		

Control ID	**SR-7**	Control Name	**Supply Chain Operations Security**
Definition	Employ the following Operations Security (OPSEC) controls to protect supply chain related information for the system, system component, or system service: [Assignment: organization-defined Operations Security (OPSEC) controls].		
IHGIN Response	OPSEC controls are implemented to protect the supply chain.		

Control ID	**SR-8**	Control Name	**Notification Agreements**
Definition	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]].		
IHGIN Response	In the case that a portion of the supply chain utilized by a customer may be subject to a system change or audit the customer will be notified of the scheduled change.		

Control ID	**SR-9**	Control Name	**Tamper Resistance and Detection**
Definition	Implement a tamper protection program for the system, system component, or system service.		
IHGIN Response	IHGIN requires tamper resistant packaging and tamper detection systems be utilized on incoming materials.		

Control ID	**SR-9(1)**	Control Name	**MULTIPLE STAGES OF SYSTEM DEVELOPMENT LIFE CYCLE**
Definition	Employ anti-tamper technologies, tools, and techniques during multiple stages in the system development life cycle, including design, development, integration, operations, and maintenance.		
IHGIN Response	This is achieved through a combination of technical and personnel control to ensure that systems development does not introduce tampered products into systems or products.		

Control ID	**SR-10**	Control Name	**Inspection of Systems or Components**
Definition	Inspect the following systems or system components [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization defined indications of need for inspection]] to detect tampering: [Assignment: organization defined systems or system components].		
IHGIN Response	IHGIN will conduct a physical inspection of systems or components when transferred through the supply chain prior to implementation or use within the environment. For example, cellular devices that have crossed an international border are inspected by IT upon return.		

Control ID	**SR-11**	Control Name	**Component Authenticity**
Definition	a) Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and b) Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].		
IHGIN Response	IHGIN utilizes anti-counterfeit mechanisms supplied by vendors to ensure that materials and software are authentic.		

Control ID	**SR-11(1)**	Control Name	**ANTI-COUNTERFEIT TRAINING**
Definition	Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).		
IHGIN Response	IHGIN receiving staff are trained to spot potential counterfeit goods and know what to expect from suppliers in terms of physical security controls in order to verify the goods as legitimate.		

Control ID	**SR-11(2)**	Control Name	**CONFIGURATION CONTROL FOR COMPONENT SERVICE AND REPAIR**
Definition	Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [Assignment: organization-defined system components].		
IHGIN Response	IHGIN maintains configuration control over system components as they await service.		

Control ID	**SR-11(3)**	Control Name	**COMPONENT DISPOSAL**
Definition	Dispose of system components using the following techniques and methods: [Assignment: organization-defined techniques and methods].		
IHGIN Response	IHGIN follows an internal destruction and disposal policy for system components and materials.		

Control ID	**SR-11(4)**	Control Name	**ANTI-COUNTERFEIT SCANNING**
Definition	Scan for counterfeit system components [Assignment: organization-defined frequency].		
IHGIN Response	Where applicable anti-counterfeit scanning is utilized through software provided by the vendor.		