EMERGENCY MANAGER CYBER SITUATIONAL AWARENESS SURVEY

EMERGENCY MANAGER CYBER SITUATIONAL AWARENESS SURVEY

INSTRUCTIONS

Below are instructions for the Emergency Manager Cyber Situational Awareness Survey. This survey was made to assist local government emergency managers who want to better assess the areas within their purview while developing and exercising their cyber emergency incident response and continuity of operations plans. This Emergency Manager Cyber Situational Awareness Survey was developed by the Indiana Executive Council on Cybersecurity, National Governors Association Cybersecurity Academy participants, as well as Indiana State University. This survey is meant to begin conversations between an emergency manager and his/her local government partners as well as provide a collective overview of the emergency manager's area through a risk profile using the information provided.

Using this survey and working with the Cybersecurity Program Director from the Indiana Department of Homeland Security and Indiana Office of Technology, an emergency manager will be provided with a comprehensive risk profile provided by the State of Indiana in partnership with Indiana State University so an emergency manager is better informed as to what he or she should be focusing on when planning for a cyber attack. All information provided to the state will be kept confidential.

Emergency Manager Cyber Situational Awareness Survey Instructions:

1. The Emergency Manager, who is the main point of contact for the state, retrieves the Emergency Manager Cyber Situational Awareness Survey PDF file online at https://www.in.gov/cybersecurity/3818.htm.
2. The Emergency Manager completes the "Emergency Management Overview" (EMO) page to document the critical infrastructure (CI) and key resource systems within their oversight.
3. Using the critical infrastructure and key resource systems identified in the EMO as a point of reference, the Emergency Manager communicates with a point of contact who is responsible for each individual CI and key resource system(s) identified, and requests they complete the survey for their area.
4. Those responsible for the CI and key resource systems complete his or her copy of the Cyber Situational Awareness Survey (CSAS). The survey can be done on the fillable PDF or completed by hand.
5. Those responsible for the CI and key resource systems send their completed survey back to the Emergency Manager.

6. Once the EMA collects all the completed surveys, he or she will send their overview survey sheet and all the surveys completed (saved or scanned) to the State of Indiana Cybersecurity Program Director Chetrice Mosley at MosleyCLM@iot.in.gov.
7. The State of Indiana, working with a secure lab at Indiana State University, will then complete an analysis and develop a custom confidential Risk Profile for each Emergency Manager.
8. The Risk Profile will then be provided to each Emergency Manager allowing them to: better inform their planning, heighten training, and create appropriate exercises for their areas of responsibility. Emergency Managers will then communicate to their leadership the current status of their cybersecurity posture and priorities.

If you have any questions, please feel free to email the State of Indiana Cybersecurity Program Director Chetrice Mosley at MosleyCLM@iot.in.gov or call her at 317-607-3178.

Emergency Manager Cyber Situational Awareness Survey

Name of County:	Name of City:
Address:	
Phone:	IDHS District:
Email Address:	Population of area supervised:

What critical infrastructure and key resource systems do you oversee as an emergency manager in your organization? Select all that apply.

Communications
County or Municipality Owned Telecommunication Services (Cable, Broadband, etc.)
Dams
Educational Facilities (K-12 School Systems)

Emergency Services	Law Enforcement 9-1-1 Operations Emergency Management Fire & Rescue Emergency Medical Services
Energy	
	County or Municipality – Ran Electricity County or Municipality – Owned Oil County or Municipality – Owned Natural Gas
Elections	

Government Facilities	
	Offices and Office Building Complexes
	Housing for Government Employees
	Correctional Facilities
	Embassies, Consulates, and Border Facilities
	Courthouses
	Libraries and Archives
Healthcare & Public Health	
	Public Health Departments
	County or Municipality Owned Hospitals or Health Facility

Political Offices

Auditor

Assessor

County Commissioner

Sheriff

Transportation Systems

Aviation

Highway & Motor Carrier

Maritime Transportation Systems

Mass Transit & Passenger Rail

Pipeline Systems

Freight Rail

Postal & Shipping

Wastewater – Publicly owned wastewater treatment systems
Water – Public drinking water systems
Other:_____________________________

CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

Organization Name:	**Name of Person Completing Survey:**
Address:	
Phone:	**Email:**

Organization Information

1. How many employees are there in your organization? ________

2. How many employees have information/technology related duties? ________

3. How many employees have cybersecurity related duties? ________

4. How many times in the last 5 years has your organization been the victim of a cyberattack? ________

Yes **No**

5. Do you have cybersecurity policies?

6. Do you outsource your cybersecurity needs?

7. Do you include security requirements in your agreements with vendors?

8. Has your organization completed a cyber assessment in the last 2 years?

CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

Voice Communications

9. What voice communication systems does your organization use? Select all that apply.

Voice Over Internet Protocol (VOIP) Telephones or Services:

Uses voice over Internet Protocol (IP) technologies for placing and transmitting telephone calls over an IP network, such as the Internet, instead of the traditional public switched telephone network (PSTN) with an analog phone.

Analog Telephones (POTS):

Voice-grade telephone service employing analog signal transmission over copper loops, aka plain old telephone service or plain ordinary telephone service.

Digital Handheld Radios:

Person-to-person two-way radio voice communications systems which use portable, mobile, base station, and dispatch console radios. These systems are used by police, fire, ambulance, and emergency services, and by commercial firms such as taxis and delivery services.

Digital Console Radios:

Same as above description but in non-mobile form.

Satellite Telephones:

Type of mobile phone that connects to other phones or the telephone network by radio through orbiting satellites instead of terrestrial cell sites, as cellphones do.

Radio over Internet Protocol (RoIP):

Like Voice over Internet Protocol (VoIP), but augments two-way radio communications rather than telephone calls.

Voice Communications (cont.)

Employer-Issued Cellular Smartphone (e.g. iPhone, Android):

Smartphone owned, issued, supported, and paid for by the employer, and the employee typically agrees to specific usage guidelines.

Personal Cellular Smartphones (e.g. iPhone, Android):

Smartphone that is owned, supported, and paid for by an individual.

Other: ___________________________________

Data Communications

10. What data communication systems does your organization use? Select all that apply.

Government Email (.gov):

The .gov top-level domain (TLD) facilitates collaboration among government-to-government, government-to-business, and government-to-citizen entities.

Commercial Email (.com/.net) (e.g. Gmail, Yahoo, iCloud):

Free web-based email service (webmail) providers. Typically accessed via web browser or smartphone app.

Wireless Local Area Network:

A wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area (WIFI).

CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

Data Communications (Cont.)

Organization Provided Internet Service:

Your company, organization, etc… is provided access to the Internet via a 3rd party Internet Service provider (ISP).

Mobile WiFi Hotspots:

An ad hoc wireless access point that is created by a dedicated hardware device or a smartphone feature that shares the phone's cellular data.

Publicly Accessible Website:

A collection of related network web resources, such as web pages, multimedia content, which are typically identified with a common domain name, and published on at least one web server. Notable examples are wikipedia.org, google.com, and amazon.com.

Organization Email (.com/.org):

A business email address / service given to an employee by the company where they work.

Wired Local Area Network:

A computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

Commercial Internet Service (Xfinity, Comcast, Spectrum):

An organization that provides services for accessing, using, or participating in the Internet.

Government Provided Internet Service:

Your company, organization, etc… is provided access to the Internet via a Government Internet Service provider, ex: Local, County, City, State of Indiana, or Federal.

Internal Network / Website (Intranet):

A computer network for sharing corporate information, collaboration tools, operational systems, and other computing services only within an organization, and to the exclusion of access by outsiders to the organization.

CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

Data Communications (Cont.)

Restricted Website (e.g. anything that uses HTTPS):

A controlled private network that allows access to partners, vendors and suppliers or an authorized set of customers – normally to a subset of the information accessible from an organization's intranet.

■ Other: ___________________________________

Data Types

11. What data types does your organization use? Select all that apply.

Sensitive / FOUO Information:

Unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national interest.

Law Enforcement Sensitive Information:

Denotes information that was compiled for law enforcement purposes and should be afforded security in order to protect certain legitimate Government interests

Protected Critical Infrastructure Information:

Critical infrastructure information means information not customarily in the public domain and related to the security of critical infrastructure or protected systems.

CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

Data Types (cont.)

Vital Public Records:

Records of life events kept under governmental authority, including birth certificates, marriage licenses (or marriage certificates), and death certificates. In some jurisdictions, vital records may also include records of civil unions or domestic partnerships.

Medical Records:

Protected health information includes all individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other information used to identify a patient or provide healthcare services or healthcare coverage.

Court Records:

The official written documentation of what happened during a trial or a hearing.

Purchasing / Contract Records:

Typical contract types include fixed-price, cost-reimbursement, incentive contracts, time-and-materials, labor-hour contracts, indefinite-delivery contracts, Bilateral, Unilateral, Express, Contract Under Seal, etc.

Credit Card Information:

Includes: Primary Account Number (PAN), Cardholder Name, Expiration Date, Service Code, Full track data (magnetic-stripe data or equivalent on a chip), CAV2/CVC2/CVV2/CID, PINs/PIN blocks.

Bank Account Information:

Includes Social Security number, Online login or password, One Time Password (OTP), Debit or credit card number, ATM card number or PIN, Routing number, Account number, Personal check, Paystub, Driver's license information, Children's personal information.

Personally Identifiable Information (e.g. social security Numbers, bank account numbers, email addresses):

Data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Other: ___________________________________

CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

Data Storage & Equipment

12. Where is your data stored and what equipment is used in organization? Select all that apply.

Organization-Managed Data Center - In-Building:

A dedicated space within a building, or a group of buildings used to house computer systems and associated components, such as telecommunications and storage systems.

Organization Data Center – Offsite:

A building, dedicated space within a building, or a group of buildings[4] offsite, used to house computer systems and associated components, such as telecommunications and storage systems

Vendor Managed Data Center – Cloud Based:

A remote version of a data center – located somewhere away from your company's physical premises – that lets you access your data through the internet.

Network Infrastructure (e.g. routers, switches, hubs):

The hardware and software resources of an entire network that enable network connectivity, communication, operations and management of an enterprise network. It provides the communication path and services between users, processes, applications, services and external networks/the internet.

Desktop Computers:

A personal computer designed for regular use at a single location on or near a desk or table due to its size and power requirements.

Tablets (iPad, Surface):

A mobile device, typically with a mobile operating system and touchscreen display processing circuitry, and a rechargeable battery in a single, thin and flat package

Secured Employee Drives:

A technology that encrypts the data stored on a hard drive using sophisticated mathematical functions

Desktop Printers / Scanners:

Personal printers are primarily designed to support individual users, and may be connected to only a single computer.

CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

Data Storage & Equipment (cont.)

Networked Printers/Scanners:

Networked or shared printers and/or scanners.

Cellular Telephones:

A portable telephone that can make and receive calls over a radio frequency link while the user is moving within a telephone service area.

Local Servers – In-Office:

A computer program or a device that provides functionality for other programs or devices.

External Hard Drives:

An external hard drive is a portable storage device that can be attached to a computer through a USB or FireWire connection, or wirelessly.

CD-ROM:

A pre-pressed optical compact disc with the capacity to hold approximately 700MB of data.

Networked Shared Drives:

A computer attached to a network that provides a location for shared disk access, i.e. shared storage of computer files (such as text, image, sound, video) that can be accessed by the workstations that are able to reach the computer that shares the access through a computer network.

Thumb Drives:

A USB flash drive -- also known as a USB stick.

Other: ___________________________________

CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

13. On a scale of 1 to 5, with 1 being least confident and 5 being most confident, how confident are you in your accounting for your organizations' voice communications, data communications, data types, and data storage and equipment?

1	2	3	4	5

Operations Impact

14. On a scale of 1 to 5, with 1 being no impact on your day-to-day operations and 5 being the most impact on your day-to-day operations (e.g. you must close), what level would your organization's operations be affected if taken down by a cyberattack?

Operation Systems	1	2	3	4	5
Voice Communication Systems	1	2	3	4	5
Email System	1	2	3	4	5
Databases of Information	1	2	3	4	5

CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

Public Safety and Health Impact **Yes** **No**

15. If your operation systems are down/compromised will the health and/or safety of the public be at risk?

16. If your information systems are down/compromised will the health and/or safety of the public be at risk?

17. If your communication systems are down/compromised will the health and/or safety of the public be at risk?

18. If your email system is down/compromised will the health and/or safety of the public be at risk?

Preparedness and Response

19. Does your organization have multi-factor authentication?

20. Does your organization install computer updates and/or patches regularly?

21. Do you install your updates and/or patches automatically?

22. Does your organization have a cyber emergency response plan in place to address a cyberattack on your organization?

CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

Preparedness and Response (cont)	Yes	No
23. Does your organization provide your employees cybersecurity awareness and/or training?		
24. Does your organization have a continuity of operations plan?		
a) If yes, does your continuity of operations plan account for a cyber attack?		
25. Are your organization's 'smart' devices (such as security cameras, thermostats, HVACs, alarm systems, etc.) periodically monitored and scanned for security vulnerabilities and malicious software?		

CYBER SITUATIONAL AWARENESS SURVEY (CSAS)

Recovery

26. In the event of a critical information system disruption or loss, what backup or redundant systems are in place for your organization?

System Types

Operation Systems	Multiple automatic backup systems are in place	An automatic or manual backup system is in place	A manual backup system is in place	Improvised system backups can be employed	No backup system is in place	I do not know
Email Systems	Multiple automatic backup systems are in place	An automatic or manual backup system is in place	A manual backup system is in place	Improvised system backups can be employed	No backup system is in place	I do not know
Information from Databases	Multiple automatic backup systems are in place	An automatic or manual backup system is in place	A manual backup system is in place	Improvised system backups can be employed	No backup system is in place	I do not know

27. On a scale of 1 to 5, with 1 being least confident and 5 being most confident, how confident are you in your preparation, response, and recovery abilities in the event of a cyberattack?

1	2	3	4	5