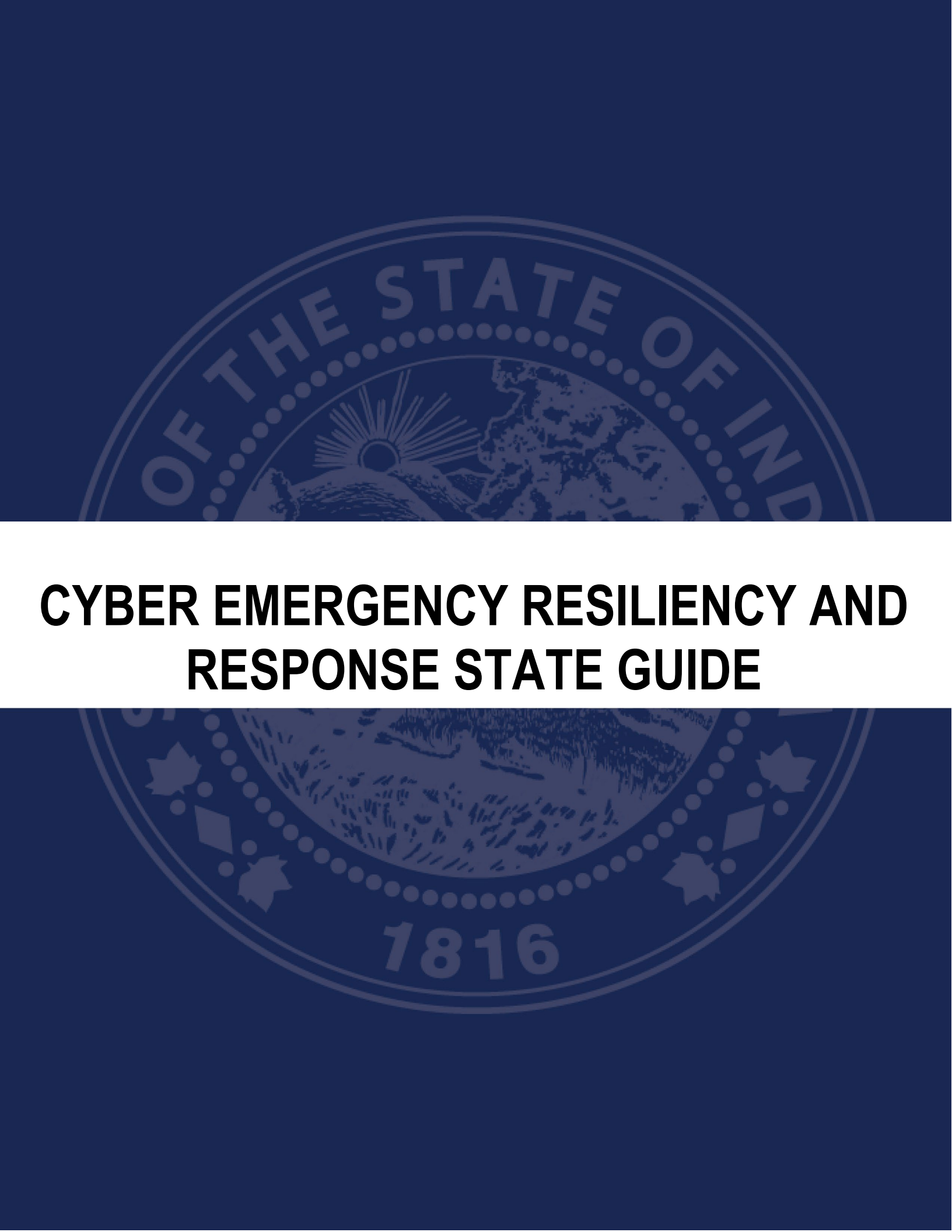


CYBER EMERGENCY RESILIENCY AND RESPONSE STATE GUIDE

CYBER EMERGENCY RESILIENCY AND RESPONSE STATE GUIDE

Table of Contents

1.0 Introduction 3
2.0 Purpose 3
3.0 Scope 3
4.0 Cyber Emergency Preparation and Response Plan Core Group 4
5.0 Cyber Emergency Preparation Process 7
6.0 Response Process 8
7.0 Plan Maintenance 8

1.0 Introduction and Definitions

The Indiana Cyber Emergency Resiliency and Response State Guide (State Guide) was created to communicate the roles of an effective emergency response to a cyber emergency from the Executive Branch of Indiana government and indicate what roles partners may have during a cyberattack.

Determining which organizations should be involved and the roles they will play has proven challenging at all levels of government for nontraditional catastrophic emergencies such as a cyber attack. Emergency managers often have a difficult time understanding the technical nature of a cyber attack and how that fits in an emergency response while still developing decision-making processes that are true to an all-hazards approach. Below are emergency management resources to assist in planning and responding to a cyber attack.

Cyber Emergency VS Cyber Incident

The State of Indiana defines a **cyber emergency** as any actual, imminent, or potential incident that will adversely affect public health, safety, or security; the environment; or economic prosperity on a level materially significant to the State of Indiana or its operations that requires a coordinated state response.

The State of Indiana defines a **cyber incident** as it is described in the Presidential Policy Directive 41, which is "an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical, or virtual infrastructure controlled by computers or information systems, or information resident thereon."

2.0 Purpose

The State Guide the roles, considerations, and process to effectively coordinate the proper resources to proactively protect and defend state-owned data systems and networks during a cyber emergency. This will also provide clarification to the state's role in assisting local units of government in a cyber-related incident as well as coordinating with private sector partners.

3.0 Scope

The State Guide will be utilized when the following criteria are met:

- A cyber emergency involving activation of state level continuity of operations (COOP), or continuity of government (COG) plans.
- A cyber event that has a material impact on public safety.
- A threat or incident involving state-level, cyber-critical infrastructure.
- When requested by:
    - A local government entity
    - Director of the Indiana Office of Technology
    - Director of the Department of Homeland Security
    - The Adjutant General of Indiana

- When directed by:
    - The Governor of Indiana

4.0 Cyber Emergency Resiliency and Response Partners

The State of Indiana relies on a core group of agencies to assess the circumstances, determine an emergency, and deliver the response needed from state government. Inclusion in the core group is driven by the essential expertise and capabilities needed from the Executive Branch to assess and potentially assist in a response to the cyber emergency situation. As with many other threats and hazards, the success of resiliency and response must rely on the state, federal, public, military, and private partners.

STATE AGENCIES AND PARTNERS

OFFICE OF THE GOVERNOR

The Governor provides overall direction and control for the preparation and carrying out of all emergency actions, including development and execution of the State's Comprehensive Emergency Management Plan. State agencies will support emergency operations in accordance with Executive Order 17-02.

INDIANA DEPARTMENT OF HOMELAND SECURITY

IDHS is tasked to coordinate the state's emergency plans, and serve as the coordinating agency for state efforts for preparedness for, response to, mitigation of, and recovery from emergencies and disasters. As with other hazard-related emergencies, IDHS manages the operations of the State Emergency Operations Center.

INDIANA OFFICE OF TECHNOLOGY

IOT oversees and manages the IN-ISAC. IOT is responsible for the security of state government information networks and all domains and is responsible for protecting the State's IT infrastructure from internal and external cybersecurity threats. IOT will assist IDHS during an cyber emergency activation with situational awareness, identifying external decision-makers, and accessing the necessary mitigation resources and lead remediation efforts if the event affected state government infrastructure.

INDIANA STATE POLICE

The ISP Office of Intelligence and Investigative Technologies (OIIT) focuses on cybersecurity incidents with a criminal nexus. The Cybersecurity Crime and Investigative Technologies Section and the Crime Analysis Section conduct activities related to cybersecurity forensics, cybersecurity crime investigations including those involving network intrusion and exploitation, electronic surveillance, and crimes against children.

The Indiana Intelligence Fusion Center (IIFC) collaborates with the IN-ISAC to conduct criminal intelligence analysis and incident reporting involving cybersecurity crimes. In the event that a criminal nexus is suspected in a cybersecurity emergency, law enforcement will investigate. Post-recovery, the IIFC may work with the IN-ISAC to help generate analytical after-action reports for external partners.

INDIANA NATIONAL GUARD

The INNG has a Cybersecurity Mission comprised of experts in both preparedness and response efforts. As with other state emergencies, IDHS Executive Director may request deployment of cybersecurity force packages to support incident response.

INDIANA EXECUTIVE COUNCIL ON CYBERSECURITY

Signed by Governor Eric. J Holcomb on January 9, 2017, the Indiana Executive Council on Cybersecurity (IECC or Council) was continued through Executive Order 17-11 with the recognition that a cross-sector body of subject-matter experts is required to form an understanding of Indiana's cyber risk profile, identify priorities, establish a strategic framework of Indiana's cybersecurity initiatives, and leverage the body of talent to stay on the forefront of the cyber risk environment.

Led by the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana State Police, and the Indiana National Guard, the Council is made up of government (local, state, and federal), private-sector, military, research, and academic stakeholders to collaboratively move Indiana's cybersecurity to the Next Level. With 35 Council members and more than 250 advisory members, the Council delivered a comprehensive strategy plan to Governor Holcomb September 2018.

Moreover, the experts of the Council are charged with providing best practices, resources, and information to increase the state resiliency against cyberattacks. In addition to the private and public partners, state agencies and elected officials such as the Indiana Economic Development Corporation, Indiana Secretary of State, Indiana Attorney General, and many more have come together to increase the resiliency.

In a cyber emergency, experts from the Council may be included as a part of the Cybersecurity Advisory Group.

CYBERSECURITY ADVISORY GROUP

The Indiana Cybersecurity Advisory Group (CAG) provides operational guidance and subject-matter expertise in support of a coordinated state cybersecurity incident response. The CAG will assess the incident and organize the strategic response to give to IDHS's Emergency Operations Center. The CAG also develops, coordinates, and recommends courses of action and response strategies. Designated agency representatives include the IOT Chief Information

Security Officer, or designee, ISP Commander, Intelligence and Investigative Technologies or designee, INNG Defensive Cybersecurity Programs Lead, or designee, Indiana Cybersecurity Program Director, IDHS Division Director, Response and Recovery, or designee and selected subject-matter experts.

FEDERAL AGENCIES

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

The Cybersecurity and Infrastructure Security Agency (CISA) is the designated lead agency during a cybersecurity incident requiring a federal response. Their primary functions are to identify the source of disruption and help remove it, determine how they gained access, assess the damage, and provide guidance to the organization on how to make their system more secure.

FEDERAL BUREAU OF INVESTIGATION

The FBI is the lead federal agency for investigating cybersecurity-attacks by criminals, overseas adversaries, and terrorists. Specially trained FBI agents and analysts based at the FBI Indianapolis Field Office investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud.

U.S. SECRET SERVICE

The Secret Service maintains Electronic Crimes Task Forces, which focus on identifying and locating international cybersecurity criminals connected to cybersecurity intrusions, bank fraud, data breaches, and other computer-related crimes. The Secret Service also runs the National Computer Forensic Institute, which provides law enforcement officers, prosecutors, and judges with cybersecurity training and information to combat cybersecurity crime.

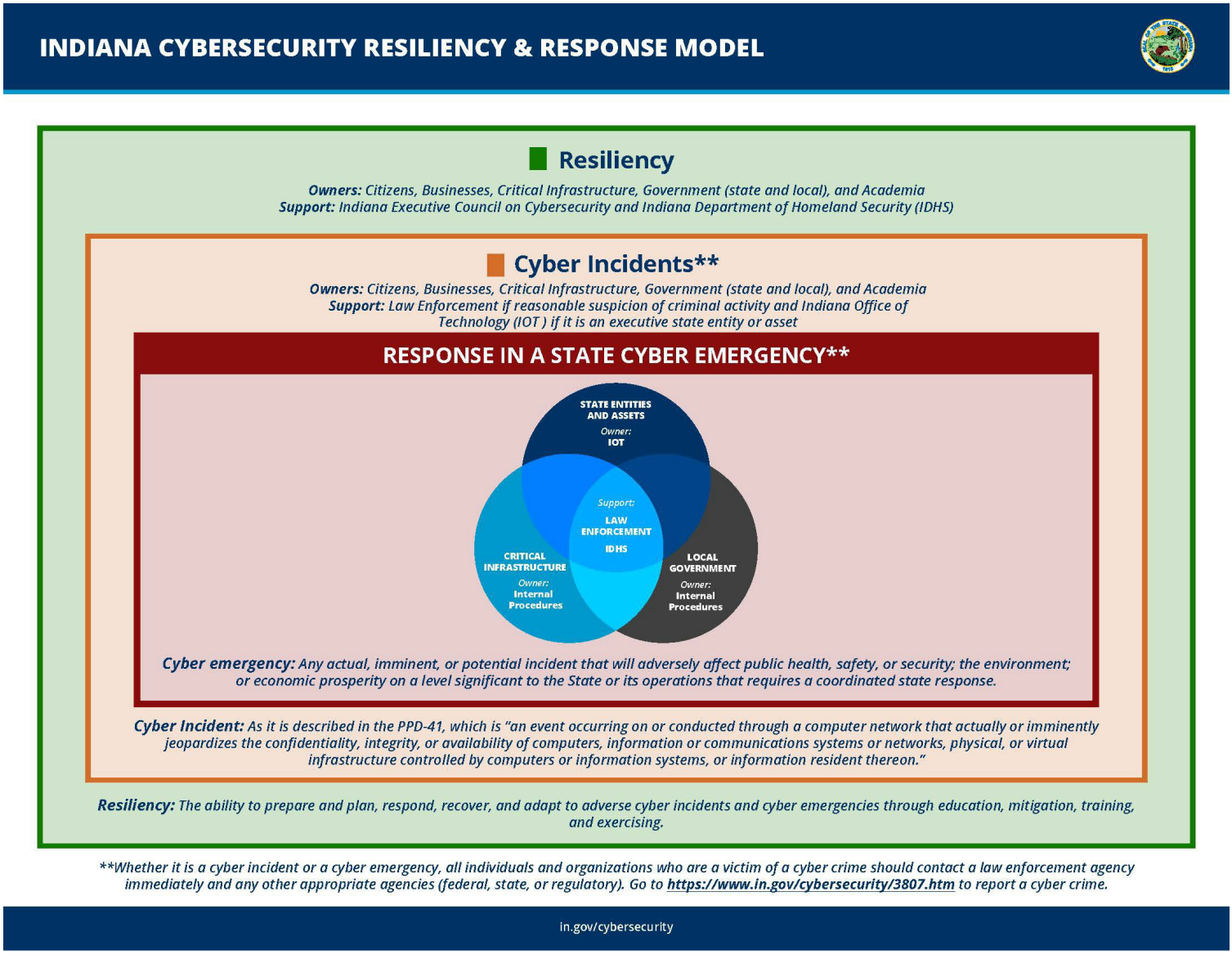
U.S. DEPARTMENT OF JUSTICE

DOJ’s Offices of U.S. Attorneys and its’ Criminal and National Security Divisions, working with federal law enforcement agencies, use criminal and national security authorities to investigate, prosecute, and disrupt cyber threats and to apprehend cyber threat actors. Information and evidence obtained pursuant to appropriate legal process are used to identify the source of cyber incidents and to gather pertinent cyber threat information.

5.0 Cyber Emergency Resiliency Efforts

The State of Indiana core agency group include the Indiana Department of Homeland Security, Indiana Office of Technology, Indiana National Guard, and Indiana State Police.

This core agency group assists and leads in the overseeing of the cybersecurity resiliency efforts of the Indiana Executive Council on Cybersecurity and the ability for the state to be prepared to enable the rapid and effective response needed by state government constituents during a cyber emergency or cyber incident as appropriate. The following Indiana Cybersecurity Resiliency and Response Model further identifies the owners and support organizations during the resiliency phase, a cyber incident, and a cyber emergency.



6.0 Response Process

It is important to note that once the State of Indiana is notified, the following process was created with a single objective: Get the emergency into the hands of capable, representative, and empowered individuals to bring Indiana government resources and relationships quickly to the aid of those suffering from a cyber emergency.

Once a request for assistance is received by one or more state agencies, the core agency group will convene and assess the traits and impacts of the cyber incident or emergency and the value of their resources as they apply to an effective response to the emergency, whether it is with state resources or working with other key public and private partners. Cyberattacks shared with the State of Indiana will stay at the highest level of leadership and only shared with need-to-know parties. After each cyber event reported to one or more of the core agency groups, a post-emergency evaluation will be completed by the state's Cybersecurity Program Director to rate response effectiveness, identify additional needs, and process adjustments.

7.0 Plan Maintenance

The State of Indiana Department of Homeland Security Executive Director, Indiana Office of Technology Chief Information Officer (CIO), and Indiana Cybersecurity Program Director are responsible for overall administration and maintenance of this State Guide.

This page is intentionally left blank