WASHINGTON MILITARY DEPARTMENT

Washington State

Significant Cyber Incident Annex

To the Washington State Comprehensive

Emergency Management Plan

Annex D

March 2015

Table of Contents

INTRODUCTION

"I know it is February 14, 2012, but I fear that when it comes to protecting America from cyber attack it is September 10, 2001, and the question is whether we will confront this existential threat before it happens?" - Senator Joe Lieberman (14 Feb 12, Senate Floor)

Cyber threats are an increasingly unpredictable, dangerous, and proliferating hazard to state, local, and tribal governments, as well as private industry and operators of critical infrastructure systems within the State of Washington. Every day, networks are under attack across the state from a variety of sources, using a variety of methods, all of which are growing in sophistication. In most cases, governments, industry, and operators of critical infrastructure are able to contain these threats and need no additional assistance for help. However, what happens when a cyber incident is not contained at the lowest level and requires increased coordination?

The State of Washington must respond to the challenges of a significant cyber event together in a "whole of government, whole of community" fashion to mitigate the cyber risks to protect critical communications, response capabilities, and critical infrastructure within the State. The Washington Significant Cyber Incident Annex (WSCIA) to the Comprehensive Emergency Management Plan (CEMP) provides a basic coordination framework similar to existing emergency management frameworks for State, Local and Tribal governments, the private sector, and operators of cyber critical infrastructure to manage a significant cyber event when it occurs. The CEMP and this WSCIA Annex is provided for all communities and emergency managers to promote interoperability at the federal, state, local, and tribal level. This WSCIA plan does not attempt to answer all of the possible questions concerning cyber response in the state, but merely provides a format and structure for a state response should an incident occur.

The rapidly converging information technology (IT) and communications infrastructure, known as cyberspace, touches every facet of human life. The United States and Washington State in particular, embrace cyberspace, using it for diverse activities from increasing energy efficiency to conducting financial transactions. President Obama recognized national reliance on cyberspace and commissioned the Cyberspace Policy Review released on May 29, 2009. This document builds on the Comprehensive National Cybersecurity Initiative (CNCI) and calls for the development of a cybersecurity incident response plan.

In August of 2012, the Washington State Committee on Homeland Security also recognized the importance of cyberspace and cybersecurity. The committee added cybersecurity as one of the seven hazards afforded formal planning study as part of the Federal Threat and Hazard Identification and Risk Assessment (THIRA) process. The recognition that cybersecurity threats can cause catastrophic consequences serves to strengthen the importance of a robust and integrated planning effort for a significant cyber incident.

Recognizing the need for an overarching policy and approach to cyber incidents occurring or directly impacting the citizens of Washington State, the WSCIA was developed according to the principles outlined in the National Response Framework (NRF) and the Draft National Cyber Incident Response Plan (NCIRP), and describes how the State responds to significant cyber incidents. While the NRF and the Draft NCIRP provide the Nation with guiding principles that enable all response partners to prepare for and provide a unified national response, the WSCIA provides guidance on how the State plans to address significant cyber issues occurring at the state, local, tribal or private sector levels.

The WSCIA is built on the foundations of the NRF and is intended to coordinate activities with NRF mechanisms during cyber incidents with physical consequences, such as disruption to the power grid or water delivery systems, among many others. Cyber incident responders at all levels are strongly encouraged to familiarize themselves with the NRF, the Draft National Cyber Incident Response Plan, and the National Incident Management System (NIMS).

Cyberspace is a modern technological realm that helps drive progress in everything from scientific innovation to international trade. The foundations of cyberspace remain vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in cyberspace can be exploited by both nation-states and non-state actors. The risks associated with the Nation and Washington State's dependence on cyberspace led to the development of the CNCI and the Cyberspace Policy Review at the Federal level and the organization of the Washington State Cyber Integrated Project Team (IPT) at the State level. The IPT has been the first conversation about cybersecurity from an integrated and whole of state perspective to date within Washington.

The WSCIA is a key product of the Cyber IPT, and is designed in full alignment with these initiatives to ensure that state cyber incident response policies facilitate both the rapid internal state-level and national coordination needed to defend against the full spectrum of threats. The WSCIA focuses on improving the human and organizational responses to cyber incidents by creating a statewide framework for significant cyber incidents, while parallel efforts focus on prevention and protection activities through outreach efforts and educational processes across state, local, tribal, and private industry partnerships in line with other emergency preparedness activities conducted by the Emergency Management Division (EMD).

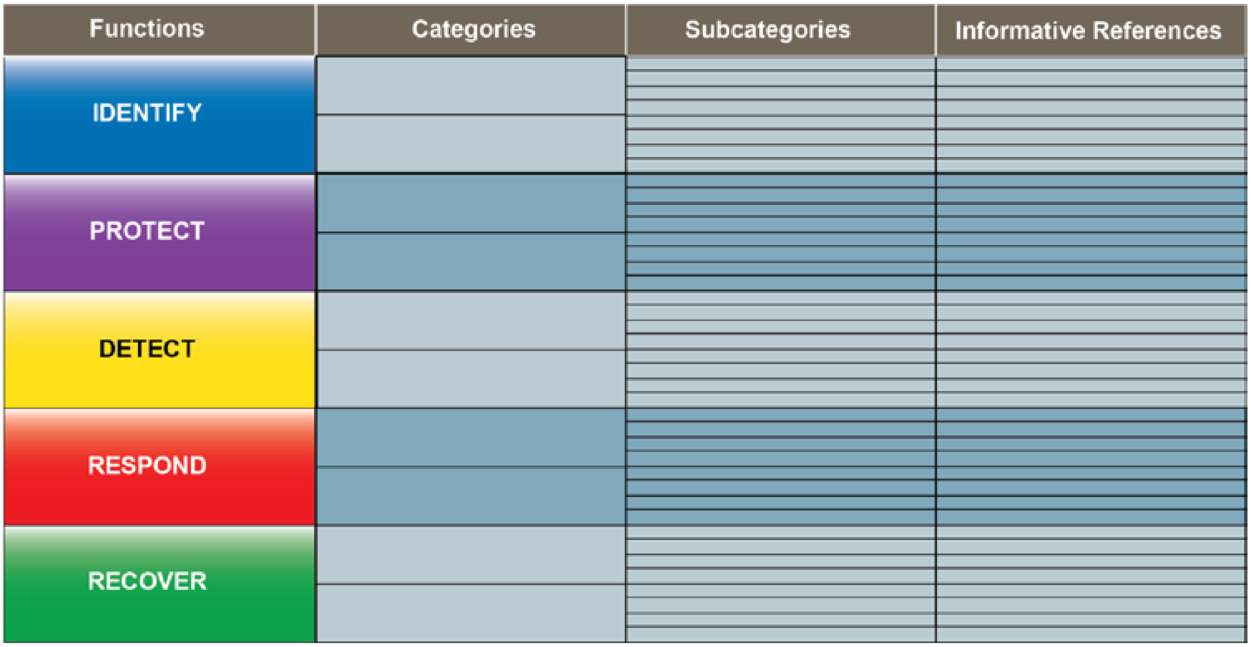
PURPOSE

"[Cybersecurity] is a matter of public safety and national security… The cyber threat is one of the most serious economic and national security challenges we face as a nation." - (President Obama, 2009)

The purpose of the WSCIA is to establish the strategic framework to prepare for, respond to, and begin to coordinate response to and recovery from a significant cyber incident. It ties various policies and doctrines together into a single tailored, strategic, cyber specific plan designed to assist with operational execution, planning, and preparedness activities and to guide recovery efforts.

In the current risk environment, cyber incidents occur daily, often cascading across federal, state, local, tribal, territorial, and private sector systems. Significant cyber incidents may require increased cooperation and coordination to reduce the effects of the event. With these interdependencies in mind, the WSCIA was developed.

The WSCIA is a strategic and operational framework for coordination and execution among federal, state, local, tribal, and territorial governments; the private sector; and operators of cyber critical infrastructure partners. Communities and emergency managers are highly encouraged to work in partnership and to refer to documents like the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity when developing individual agency or organizational cyber incident response plans.



Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Figure 1: NIST Cyber Security Core Framework

Detailed operational plans support the WSCIA at the state agency, local government, tribal and private sector levels. In all cases, incident response activities will be conducted in accordance with applicable law and policy and nothing in this plan restricts, supersedes, or otherwise replaces the legal authorities or regulatory responsibilities of any government agency or organization. All information will be handled, transmitted, distributed, released, and/or stored in accordance with the standards, caveats, and procedures described by the originating agency, regulatory governance, and/or law.

SIGNIFICANT CYBER INCIDENT

A significant cyber incident is defined in this CEMP as an event that is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public safety, undermine public confidence, have a negative effect on the economy, or diminish the security posture. State-level coordination of significant cyber incidents is triggered when the State Emergency Operations Center (SEOC) activates after receiving a request for assistance related to the incident. At that point, the significant cyber incident will be monitored and coordinated through the SEOC under the guidance of the Cyber Unified Coordination Group (UCG), which is described below. The Governor may proclaim a state of emergency under RCW 43.06.010(12) and/or order the National Guard into active state service under RCW 38.08.040 in response to the incident.

The Governor of Washington has designated the Homeland Security Advisor (HSA) to manage a significant cyber incident within the State of Washington. HSA has determined that during a significant cyber incident triggering state-level coordination, the proper coordination mechanism is a Cyber UCG, which is discussed in greater detail below. During a significant cyber incident triggering state-level coordination, the SEOC, under the guidance of the UCG, coordinates state cyber response efforts and works directly with federal, state, local, tribal, and territorial governments and private sector partners.

Examples of significant cyber incidents that may trigger state-level coordination are those that impact transportation management; public safety communications; emergency response capability; drinking water; waste removal and processing; energy delivery; monetary actions; telecommunication systems; exploitation of data for monetary loss; critical infrastructure and key resources (CIKR) sectors.

ORGANIZATION DURING A SIGNIFICANT CYBER INCIDENT

There are a number of key players with roles and responsibilities during a significant cyber incident. Some of these individuals or organizations are described in greater detail below.

Homeland Security Advisor (HSA)

During a significant cyber incident, the State of Washington HSA reports directly to the Governor with responsibility for coordinating significant cyber incident related activities for the State of Washington.

Cyber Unified Coordination Group

Required resources, authorities, and execution responsibilities do not reside in one department, agency, organization, or company within the State of Washington. The HSA coordinates significant cyber incident response efforts with the help of the Cyber UCG. The Cyber UCG consists of carefully selected representatives from federal, state, and local governmental agencies, academia, and representations from private industry and critical infrastructure sectors that can quickly acquire resources, authorities, and information for a coordinated response to a significant cyber incident.

Participants in the Cyber UCG use their own authorities to assist response activities and are responsible for understanding and communicating the full range of capabilities that their organization brings to bear. The Cyber UCG will activate when notified by HSA, or designee, and serves as the Multi-Agency Coordination Group (MACG) body during SEOC activation.

The exact composition of the Cyber UCG shall be specific to each significant cyber incident and will be determined by the HSA or designee in coordination with select members of the Cyber UCG based on the nature and scope of the incident. The Cyber UCG includes the following members and can be expanded as necessary based on the location and circumstances of the significant cyber incident:

- HSA or designated representative
- State Office of the Chief Information Officer (OCIO) or designated representative

- Consolidated Technology Services (CTS) Director or designated representative
- Director of Emergency Management or designated representative
- Chief Information Security Officer, Washington State
- Chief Information Security Officer, City of Seattle
- Federal Bureau of Investigation (FBI) Joint Cyber Task Force representative
- Co-Chair Telecommunications & Energy, Affiliated Tribes of Northwest Indians
- University of Washington Center for Information Assurance representative
- Private Industry/CIKR representative (s) (from each of the 18 sectors depending on the specific nature of the incident)
- Washington State Emergency Management Division's Cyber Security Manager
- National Guard Lead Cyber Planner
- Washington State Patrol High Tech Crimes Unit representative
- Cyber Intelligence Analyst, Washington State Fusion Center
- Cyber Incident Response Coalition and Analysis Sharing (CIRCAS)
- Other organizations/vendors who participate in information sharing and assistance

Each department and agency involved in a significant cyber incident shall be responsible for ensuring the availability of its representative to the Cyber UCG. Cyber UCG representatives should have familiarity with both emergency and incident management processes, as well as have a deep understanding of cyber threat and response issues.

During a significant cyber incident, the HSA along with the members of the Cyber UCG will provide guidance to the Disaster Manager and SEOC Supervisor. Examples of SEOC activities include:

- Establishing the incident action plan
- Ensuring overall coordination of significant cyber incident management and resource allocation activities
- Facilitating interagency conflict resolution or elevating matters, as necessary
- Coordinating response between multiple cyber incidents when applicable
- Ensuring the Governor's Office and SEOC receive timely updates on the status of response activities
- Coordinating external affairs activities

When activated and depending on circumstances, the Cyber UCG may find it beneficial to meet at the Washington State Fusion Center (WSFC) in the FBI building in downtown Seattle. The WSFC hosts a number of classified and unclassified network feeds that will greatly enhance the UCG's abilities to coordinate a significant cyber incident.

SIGNIFICANT CYBER INCIDENT RESPONSE PROCESS

Cyberspace is a cross-sector, multi-jurisdictional operational domain that is heavily dependent on private sector owners and operators. Effective response requires close coordination across traditional boundaries and requires the development of a robust common operational picture during significant cyber incidents as a foundational element.

Effectively understanding risks in cyberspace requires that a wide range of departments, agencies, and organizations collaborate on a daily basis to share information and identify threats, vulnerabilities, and potential consequences. Cybersecurity partners should build upon regional, functional, and national efforts such as the Multi-State Information Sharing and Analysis Center (MS-ISAC) and other ISACs to build a more robust common operational picture capable of bringing together federal, state, local, tribal, and territorial resources; CIKR; and private sector perspectives. ISAC partnerships can leverage NCCIC and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) resources for consultation, analysis, or response from a fly-away team if necessary.

The Department of Homeland Security (DHS) integrates and maintains a national common operational picture for cyberspace via the NCCIC. The NCCIC provides situational awareness across cyberspace, including a continuously updated, comprehensive picture of cyber threats, vulnerabilities, and consequences to provide indications and warning of imminent incidents, and to support a coordinated incident response. Regional monitoring such as the Public Regional Information Security Event Management (PRISEM) system and well-established contacts with various ISACs can provide real-time access to cyber event and incident alerts across the State of Washington. With access to the system provided to a Cyber Intelligence Analyst, programs like PRISEM can supply situational awareness regarding the threat surface of a region, and provide a common operating picture across the participating public, energy, and health-sector organizations.

Information updates during a significant cyber incident should be distributed to appropriate parties at the appropriate level of detail and classification by the SEOC once the UCG has been initiated. Information updates may also be provided to the National Infrastructure Coordinating Center (NICC) and the National Operations Center (NOC) to enhance the national common operating picture for the President; Secretary; Federal, State, Local, Tribal, and Territorial homeland security partners; private sector; and nongovernmental organizations (NGO) as needed.

Information for the common operational picture may come from partnerships and information sharing initiatives with the following:

- Federal departments and agencies
- The national security community and Intelligence Community (IC)
- The law enforcement community, including Federal, State, and Local law enforcement agencies
- Various public and private sector sources, such as ISACs, PRISEM and private sector companies
- Cybersecurity vendors
- Cybersecurity professionals from local governments, municipalities, ports, and public utility companies
- Open sources, such as presentations from cyber risk-related conferences

Although this common operational picture is a foundation for cyber incident response activities, effective response operations in cyberspace require the coordination and execution of a wide variety of legal and operational authorities. These activities will be centrally coordinated but executed in a decentralized fashion based on organizational responsibilities.

While working together, UCG partners should develop and share tips, indicators, warnings, information, and mitigation recommendations using established communication channels.

CENTRALIZED COORDINATION, DECENTRALIZED EXECUTION

The federal government and the State of Washington have developed legal authorities that are similarly decentralized. Each incident response partner has capabilities, authorities, and legally-mandated roles to play in securing cyberspace. These authorities have traditionally been executed without coordination, but as noted in the National Cyberspace Policy Review and confirmed by experience, the status quo is no longer acceptable. The threats and risks to the State's information and communications technology infrastructure pose a threat to public safety and security and may require the state emergency management capabilities and processes to synchronize preparedness and response efforts from multiple organizations.

GENERAL ROLES AND RESPONSIBILITIES FOR CYBER INCIDENTS

A significant cyber incident may rapidly spread across interdependent and cross-jurisdictional networks, and become significant enough to quickly require nationally-coordinated response actions based on differing authorities and priorities. The WSCIA provides the mechanisms and SEOC provides the facilities to coordinate state response efforts. The following organizations will also play key roles in this coordinated effort and will bring their authorities and capabilities to bear during a significant cyber incident.

Office of the Governor (GOV):

In accordance with RCW 38.52.030(2) & (3) and RCW 38.52.050, the Governor provides overall direction and control for the preparation and carrying out of all emergency actions authorized under ch. 38.52 RCW, the Emergency Management Act, including development and carrying out of the State's comprehensive emergency management program. This includes preparation for and carrying out all emergency functions to mitigate, prepare for, respond to, and recover from emergencies and disasters from all hazards, whether natural, technological, or human caused, resulting from an event or set of circumstances that either (1) demand immediate action to preserve public health, protect life and public property, or to provide relief to any stricken community overtaken by such occurrences, or (2) have resulted in the Governor proclaiming a state of emergency pursuant to RCW 43.06.010(12). The Governor consults a MACG in performing these functions.

Under RCW 38.08.040, the Governor is also authorized to activate the National Guard to perform such duty as deemed proper in the event of a public disaster; when required for public health, safety or welfare; or to prepare for or recover from such events.

The Emergency Management Division (EMD):

The Director of EMD ensures the state is prepared to deal with any disaster or emergency by administering the program for emergency management delineated by the HSA. The EMD Director is also responsible for coordinating the state's response in any disaster or emergency.

Also, within EMD is the Washington State Enhanced 9-1-1 (E911) Program which facilitates local planning and installation of cyber systems to ensure the E911 system is operational and available. The State E911 Coordination Office maintains an overarching enterprise Incident Response Plan (IRP) for working with and supporting public safety answering points (PSAP) experiencing E911 outages. All jurisdictions and PSAPs must also create and maintain local IRPs for this unique system.

State Emergency Operations Center (SEOC)

As the central state point for developing and maintaining the common operational picture for emergency management efforts and working with all partners to facilitate coordination of state and national cyber response efforts, the SEOC is in a unique position to assist incident management for significant cyber incidents at the state level that require a coordinated state and national response. Therefore, the SEOC is the primary platform for coordinating operational response activities including incident prioritization, critical resource allocation, and situational awareness for issues arising as a result of a significant cyber incident. This coordination includes communicating significant cyber incident related situational awareness and activities to SEOC partners, the Governor's office, NCCIC, and the HSA to monitor and prepare for the possible onset of any further consequences.

If needed partners are not present during the onset of a significant cyber incident, the SEOC maintains the capability to physically or virtually add additional federal, state, local, tribal, territorial, and private sector partners, including international stakeholders as appropriate, to the coordinated SEOC effort. Affected partners, and those that can contribute to the response effort and risk mitigation activities, can be physically co-located and virtually connected to coordinate significant cyber incident response efforts with the SEOC and Cyber UCG.

Washington State Fusion Center (WSFC)

During a Significant Cyber Incident, the WSFC is in a unique position to facilitate information sharing using Homeland Security Information Network (a national secure and trusted web-based portal for information sharing and collaboration) cyber security alerts. During a significant cyber incident, WSFC may host the Cyber UCG when activated, and will generate cyber alerts to notify federal, state, regional, local, tribal and private sector partners with early warning indicators and potential actionable intelligence measures. Further, the WSFC is positioned to compliment Cyber UCG, NCCIC and Seattle FBI Joint Cyber Task Force notifications and updates as well as communicating and collaborating with the SEOC and WSFC cyber stakeholders. In addition, the WSFC engages with other national homeland security fusion center cyber programs through the Cyber Intelligence Network (an outreach network of corporate security, information security and intelligence community professionals) to augment the SEOC common situational awareness of a significant cyber incident.

FBI Joint Cyber Task Force (CTF)

The mission of each of the FBI's Cyber Task Forces (CTF) is to synchronize domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions. CTFs are modeled after Joint Terrorism Task Forces where one is located in each of the FBI's 56 domestic field offices. CTFs are the principal platform for cross-program collaboration in field offices on cyber topics. Cross-programmatic collaboration between FBI Computer Intrusion Program (CIP) personnel (includes special agents, intelligence analysts, and computer scientists) and personnel from the FBI's Counterterrorism, Counterintelligence, Weapons of Mass Destruction, and Criminal programs ensure that opportunities are fully identified and exploited through the development of joint strategies and joint operations. CTFs are designed and intended for multi-agency participation including federal partners, state and local law enforcement, homeland security resources, and state OCIO. FBI Cyber Division also envisions a role for the private sector within CTFs and is developing a model and guidance to facilitate this collaboration.

FBI CTF's investigate cyber intrusions, espionage, terrorism, and state sanctioned crime using the following authorities:

- USC Title 18 (Predication)
    - Criminal Investigation
    - Counterintelligence / Counter Terrorism Investigation
    - Critical Infrastructure
- USC Title 50 (National Security)
    - Intelligence Collection
    - Counterintelligence
    - Foreign Intelligence Surveillance Act (FISA)
- Executive Order 12333
    - Overseas Clandestine Operations
- NSPD-54/HSPD-23
    - Monitoring
    - SIGINT (per National Security Agency policy interpretation)

The Washington State Patrol (WSP):

The Washington State Patrol (WSP) is a professional law enforcement agency that routinely partners with other law enforcement, traffic safety, and criminal justice agencies to provide public safety services to the citizens of Washington State. WSP has the responsibility to investigate cybercrimes committed on state property, against state agencies, and against state assets. The High Tech Crimes Unit (HTCU) is a full time computer forensics team within the WSP responsible for the investigation of these crimes. The unit may also investigate cybercrimes in local jurisdictions at the request of a local law enforcement agency.

Due to the pervasive nature of cyberspace, criminal activities can cross multiple law enforcement jurisdictions complicating efforts to investigate and prosecute cybercrimes. During a significant cyber incident, WSP will coordinate the initiation of cybercrime investigations with appropriate state and local law enforcement agencies and support from our federal partners. HTCU will ensure the Cyber UCG and SEOC are aware of which law enforcement agencies are engaged. A timely response by law enforcement is critical as evidence of cybercrimes can be erased through incident response and recovery processes.

Security Operations Center (SOC):

The state of Washington Security Operations Center (SOC), located in CTS, leads the coordination and response efforts in assessing and managing cyber incidents affecting the state government networks. The SOC determines the level of response required to respond to incidents and directs the utilization of agency resources to minimize incident exposure. The SOC team is comprised of certified experts in incident handling, forensics, and penetration testing. The SOC ensures appropriate enterprise protection controls are deployed; communicates information regarding the incident to organizational partners, and keeps executive leadership informed. If a state entity does not have internal resources to respond to an incident, the SOC will handle the incident on behalf of the entity.

CIKR Sector Specific Agencies (CIKR/SSA):

In accordance with their responsibilities under the National Infrastructure Protection Plan (NIPP), CIKR/SSAs will develop a process to facilitate real-time cyber incident notification within their respective sectors and provide mechanisms for reporting this information to the SEOC. CIKR/SSAs manage the overall process for building partnerships and leveraging CIKR security expertise, relationships, and resources within their sector and are responsible for coordinating sector-level participation in the WSCIA, including supporting sector efforts to align cyber preparedness and response efforts with the WSCIA. CIKR/SSAs and sector-designated operational entities may also communicate sector priorities and protective actions in the event of widespread impact to a sector. In addition to relationships within their sector, representatives of all sectors may coordinate directly with EMD.

Regional Organizations and Working Groups:

The Cyber Incident Response Coalition and Analysis Sharing (CIRCAS) group is a regional organization that is similar to the ISAC model, used with sector-specificity at the federal level. However, CIRCAS is focused on information sharing and analysis between members, which include federal law enforcement (FBI, Secret Service), state, local, and tribal governments, and many private-sector companies in Washington State.

CIRCAS members share information on threats observed on member networks, and have a standing agreement to assist with analysis and response for those events that exceed the response capability of a member organization.

Similarly, the CIRCAS charter includes a provision for the organization to supply members as resources in the event of a regional disruption event; members of CIRCAS may be called upon to provide advice to the UCG or support to ESF2 activities during SEOC activation. This is a private-sector analog of the mutual aid mechanism that is commonly exercised and utilized during emergency operations.

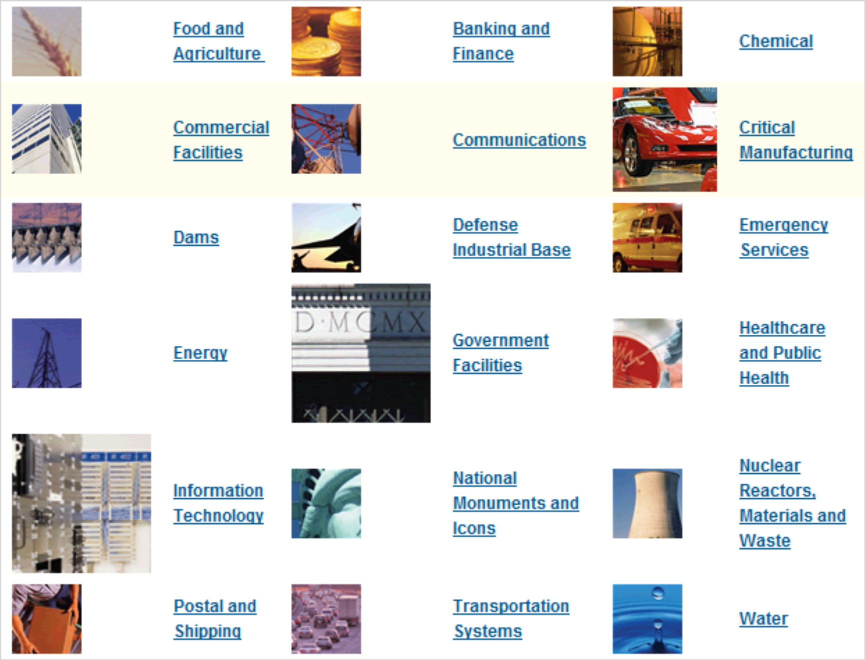


Figure 2: National Critical Infrastructure/Key Resource Sectors

Other State Agencies:

CTS is responsible for coordinating and responding during a cyber incident impacting state government agencies.

Local and Tribal Governments:

Each Chief Executive of a Local or Tribal government is responsible for its cybersecurity preparedness, response, and recovery procedures. These responsibilities should include identifying primary and secondary cyber incident response points of contact for each Chief Executive's respective government.

Multi-State Information Sharing and Analysis Center (MS-ISAC):

The MS-ISAC is a key resource for State, Local, and Tribal government information sharing, early warnings and alerts, mitigation strategies, training, and exercises and for maintenance of overall cyber situational awareness.

In addition to providing resources and assistance during a significant cyber event, MS-ISAC provides numerous types of resources to assist state and local government in responding to cyber incidents that do not rise to the level of a significant cyber event.

Private Sector:

The private sector is made up of two primary groups: (1) private sector CIKR owners and operators and (2) the general private sector. Representatives from both groups are encouraged to coordinate and communicate directly with the UCG.

CIKR owners and operators will be integrated both physically and virtually into the UCG during response actions during a significant cyber incident affecting their sector. As key owners, operators, and leaders in cyberspace and as a key part of UCG operations, CIKR owners and operators are likely to be called upon to assist the State Government during a significant cyber incident.

Other ISACs:

Multiple ISACs will provide information during a significant cyber incident. By definition, ISACs are CIKR sector-specific, trusted communities of security specialists that identify, analyze, and share information; collaborate on threats, incidents, vulnerabilities, and best practices; and generally work to protect their respective industries from cyber and physical threats. Sectors and industries without ISACs should engage with their sector specific agencies, sector coordinating council, or sector-designated operational entities to share information in a manner that is most effective for their sector.

In addition, many state and local government agencies and private sector companies have established organizational watch and warning centers. These functions may manifest themselves as security operations centers, network operations centers, or computer emergency response teams (CERT), but they all promote connectivity and security of their respective networks, as well as provide a coordinate means at the incident level. Elements inside the NCCIC work with operators of these entities to maintain accurate, up-to-date information on cybersecurity threats and vulnerabilities in order to facilitate communications during a cyber incident.

Non-Governmental Organizations (NGOs):

NGOs can provide assistance as needed and requested. They can help develop and implement sustainable strategies for effectively mitigating and addressing the consequences of a cyber incident and can provide essential services and expertise. These may include ad-hoc groups that come together to address a specific problem or well-established groups that have operated for years. The UCG and SEOC will work with its partners to identify NGOs to engage with and to develop engagement plans and coordination mechanisms for these relationships as needed.

List of Acronyms:

CIKR Sector Specific Agencies (CIKR/SSA)
Comprehensive Emergency Management Plan (CEMP)
Comprehensive National Cybersecurity Initiative (CNCI)
Computer Emergency Response Teams (CERT)
Computer Intrusion Program (CIP)
Consolidated Technology Services (CTS)
Critical Infrastructure and Key Resources (CIKR)
Cyber Incident Response Coalition and Analysis Sharing (CIRCAS)
Cyber Task Forces (CTF)
Department of Homeland Security (DHS)
Emergency Management Division (EMD)
Enhanced 9-1-1 (E911)
Federal Bureau of Investigation (FBI)
Foreign Intelligence Surveillance Act (FISA)
High Tech Crimes Unit (HTCU)
Homeland Security Advisor (HSA)
Incident Response Plan (IRP)
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
Information Technology (IT)
Integrated Project Team (IPT)
Intelligence Community (IC)
Multi-Agency Coordination Group (MACG)
Multi-State Information Sharing and Analysis Center (MS-ISAC)
National Cyber Incident Response Plan (NCIRP)
National Incident Management System (NIMS)
National Infrastructure Coordinating Center (NICC)
National Infrastructure Protection Plan (NIPP)
National Institute of Standards and Technology (NIST)
National Operations Center (NOC)
National Response Framework (NRF)
Nongovernmental Organizations (NGO)
Office of the Chief Information Officer (OCIO)
Public Regional Information Security Event Management (PRISEM)
Public Safety Answering Points (PSAP)
Security Operations Center (SOC)
State Emergency Operations Center (SEOC)
Threat and Hazard Identification and Risk Assessment (THIRA)
Unified Coordination Group (UCG)
Washington Significant Cyber Incident Annex (WSCIA)
Washington State Fusion Center (WSFC)
Washington State Patrol (WSP)