CYBERSECURITY GUIDE

for Critical Infrastructure for the State of Washington

This guide was produced by the Energy Sector Cybersecurity Working Group, a collaborative effort composed of staff of the Washington State Utilities and Transportation Commission, Washington State National Guard, Washington State Emergency Management Division, State of Washington Office of the Chief information Officer, Pacific Northwest National Laboratory (PNNL) and Snohomish County Public Utility District (PUD). This is a living document and will be updated as needed. Special thanks are due to the following people whose insights, advice and edits were indispensable:

Rebecca Beaton, Senior Analyst, Washington Utilities and Transportation Commission

Benjamin Beberness, Chief Information Officer, Snohomish County PUD

Mike Hamilton, Cyber Security Policy Advisor, Washington State Office of the CIO

Gordon Matlock, Cyber Practice Lead, Bridge Partners Consulting

Jessica Matlock, Director of Government Relations, Snohomish County PUD

Matthew Modarelli, Cyber Security Manager, Washington State EMD

Lt. Colonel Tom Muehleisen, J36 Cyber Plans and Operations, Washington National Guard

Steve Stein, Director, NW Regional Technology, Pacific Northwest National Laboratory

Troy Thompson, Chief Information Security Officer, Pacific Northwest National Laboratory

Table of Contents

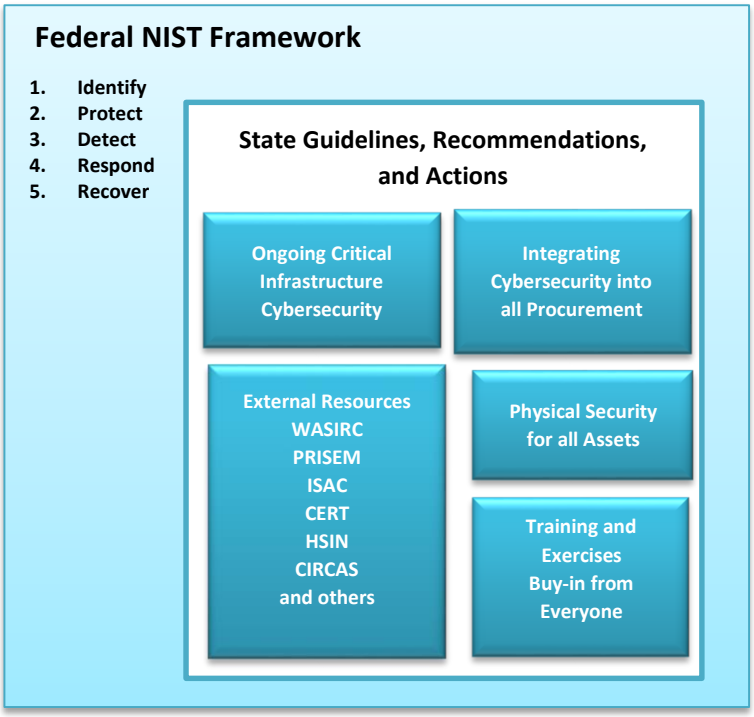
Contents

Cybersecurity Guide for the State of Washington Critical Infrastructure

"This is a matter of public safety, not just embarrassment or inconvenience. It requires a total community effort to stay ahead of those who want to do us harm." Gov. Jay Inslee, April 7th Cyber Executive Seminar, Camp Murray, WA

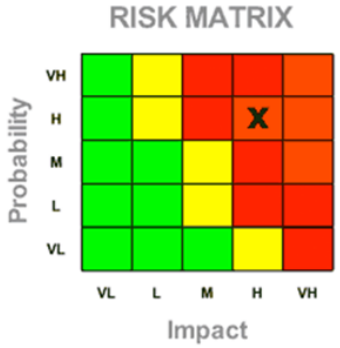
Executive Summary

The safety and economic security of the state of Washington depends on the reliable functioning of critical infrastructure such as energy delivery systems. Cybersecurity threat actors may exploit the increased complexity and connectivity of these systems, placing the state's security, economy, public safety and health at risk. Similar to financial and reputational risk, cybersecurity risk affects a company's financial health. It can drive up costs, impact revenue, and harm an organization's ability to innovate and to gain and maintain customers.



To address these risks, the following *Cybersecurity Guide for the State of Washington Critical Infrastructure* was created to provide a starting block for cybersecurity and resource information to those responsible for critical infrastructure. Using the National Institute of Standards and Technology (NIST) framework developed in response to Presidential Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, this guide describes the cybersecurity challenges and uses the NIST framework to assist critical infrastructure in establishing the planning and management of cybersecurity activities: **Identify** the risk environment, **Protect** what is important, **Detect** events that indicate a compromise of assets, **Respond** to attacks, and **Recover** your technology to an operational state and resolve any security issues.

This guide provides an overview of the NIST Framework Core Functions and Outcome Categories and the steps required to perform overall cybersecurity planning. Planning and practicing good cybersecurity requires:



- Educating and obtaining support from executives
- Identifying what is important to your business
- Identifying the risks to your business and creating protection strategies
- Developing security and acceptable cyber-asset use policies
- Conducting regular security awareness training for the company
- Developing an incident response and recovery process

Today, preventive controls such as firewalls, intrusion prevention systems, URL filtering, desktop anti-virus and email security have become less effective. Threat actors routinely use attacks that are not detected by perimeter or signature-based technologies, are more undistinguishable by using encryption and obfuscation, and rely more on social engineering (i.e., employee gullibility) than brute force attack methods. Your organization's ability to quickly detect, effectively respond to, and recover from an intrusion is critical to limiting damage and loss.

Security is not solely the domain of highly-specialized analysts. Security is the responsibility of every member of your organization and should be discussed in the same manner employee safety is handled. There are questions everyone (employees, contractors, vendors and executives) should know the answers to:

- Who in my organization is responsible for cybersecurity?
- What are the rules that govern my use of company resources (computers, smartphones and tablets)? How can I be kept aware of updates to these rules?
- If I suspect I have a cybersecurity issue (e.g., phishing, vishing, malware or spyware), who should I contact within my organization?
- How will the greater community and the state manage large-scale cyber emergencies and how do I align my agency to ensure continuity and support?
- Does my organization have a policy on bringing personal devices into the workplace?
- What am I allowed to connect to my company's system? Could my device infect the system?
- How do we create a business case to justify these costs?

Some of the best resources available are your peers from within and even outside of your industry. Trade associations and other forums (see appendices) provide the opportunities to share best practices and learn what other organizations are undertaking. These external groups/agencies can be a resource on everything from the latest threat information to sample questions for vendors within your industry or region. Information sharing conducted through trusted relationships is critical. Capabilities and expertise to respond to a cyber disruption must be available and in place prior to any event.

Finally, thinking about cybersecurity from the initial stages of the procurement process assures the business has security "baked in" and not "bolted on." Cybersecurity protections should be implemented through all phases of the product life cycle and the broader business cycle, improving reliability and reducing risks.

At the end of this guide are listings and descriptions of the State, Federal and other organizations that are resources for helping you with cybersecurity threats. Take advantage of them.

Thank you and we hope the *Cybersecurity Guide for the State of Washington Critical Infrastructure* provides assistance with making your company more secure.

The Energy Sector Cybersecurity Working Group

1. OVERVIEW

The NIST framework is an excellent resource to help organizations with their cybersecurity program. The *Cybersecurity Guide for the State of Washington Critical Infrastructure* provides some best practices at a high level to help organizations get educated and kick start their cybersecurity programs. Additionally, appendices are included for specific information and best practices for individual critical infrastructure.

NIST has identified five Framework Core Functions that are defined below. These Functions are not intended to form a serial path, or lead to a static desired end state. Rather, the Functions can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk. Each Function has several outcome Category examples associated with it.

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome categories within this Function include Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome categories within this Function include Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome categories within this Function include Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome categories within this Function include Response Planning, Communications, Analysis, Mitigation, and Improvements.

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome categories within this Function include Recovery Planning, Improvements, and Communications.

The following sections are designed to help get your organization in the right mind set and provide some high level guidance to start you on your cybersecurity journey.

2. INSTITUTIONALIZE CYBERSECURITY

It is important to not treat security as the domain of highly specialized practitioners; rather, security should be an issue that is discussed openly, frequently, and with the entire organization. For example, in many organizations safety programs are critical to ensuring a safe working environment for their employees. Every individual may have to go through safety training, they see safety posters everywhere, and they have safety incident reporting processes. Basically, safety is part of every work process and

people do not think about it as something separate from getting the job done. Cybersecurity should be treated the same way.

Executive Sponsorship and Engagement

- Critical to the success of designing a culture of security is sponsorship at the executive level. Periodic communications regarding security from the CEO, CFO, CRO, CTO, or other board- or cabinet-level executives will create and continue the perception of engagement and support for security as a cultural value in the organization.

Create a Culture

- Ensure that security is integrated into key organizational processes: hiring, procurement, job descriptions, performance metrics and termination.
- Conduct routine messaging on the importance of cybersecurity, how to resist targeted attacks, and appropriate Internet behavior and activity.

Focus on the Human

- Train and test staff regularly and repeatedly so that they understand and fully appreciate their role in maintaining a cyber-safe work environment.
- Focus on individuals with privileged access to sensitive, valuable or critical information assets.
- Institute strong security rules for vendor access to systems, facilities and equipment.
- Develop strong policies concerning employee access to sensitive information, especially at separation of employment.

3. THE BASIC RULES

There are some basic rules all organizations should follow in practicing good cybersecurity:

- Educate and obtain support from executives.
- Identify what is important to your business:
    - Create an inventory of your organization's systems and business processes, then start prioritizing.
        - Which systems and functions are most critical for meeting the mission of the business?
        - Which data systems house your company’s most sensitive information?
- Identify the risks to your business and create protection strategies.
- Develop security and acceptable asset use policies such as:
    - Providing every user with their own account with particular rights and restrictions limited to what the employee needs to perform their job duties.
    - Requiring users to have strong passwords and prompt them to update those passwords at regular intervals.
    - Updating security patches on software regularly.
    - Removing or replacing older versions of software.
    - Monitoring security logs and data for suspicious events.
    - Performing third-party security assessments (i.e., penetration tests, vulnerability testing, etc.).

    - Applying good security oversight to third parties providing products or services (limit and monitor access, require product maintenance, etc.).
- Conducting regular security awareness training for the company.
- Developing an incident response and recovery process.

The SANS Institute has created a guide for *Critical Security Controls* that provides the public with high-value action items to implement in order to maintain safe computer networks and systems (http://www.sans.org/critical-security-controls/).

4. SHARE INFORMATION

Some of the best resources out there are your peers. Trade associations and other forums can provide the opportunity for sharing best practices and learning what other organizations are undertaking. National and state organizations like the American Water Works Association (AWWA), Association of City and County Information Systems (ACCIS), Washington Association of Sewer and Water Districts (WASWD) and others have actively engaged their members on issues of cybersecurity. These groups can be a great resource on everything from the latest threat information to sample questions for vendors within your industry or sector.

Information sharing is also conducted through trusted relationships, and in fact these will be critical when the time comes for a regional response to a disruption event. Schedule and attend periodic information sharing meetings with your professional colleagues, and use the opportunity to share practices and information on events, incidents and identified threats.

Several organizations and services exist specifically to facilitate information sharing and provide a mechanism to communicate observations that may prove vital. (See appendices for resources.)

If an incident has resulted in financial loss, disruption of infrastructure, or is suspected to be the work of terrorist or nation-state actors, that information should be reported to law enforcement. Although local law enforcement does not currently have the capability of responding, the Federal Bureau of Investigation, U.S. Secret Service and other federal agencies are well-equipped and at the ready to investigate these types of incidents and offer technical recovery assistance. A law enforcement contact list for Washington state and federal agencies is included in the appendices to this document.

5. CONDUCT RISK MANAGEMENT

From the NIST *Framework for Improving Critical Infrastructure Cybersecurity* page 12:

> *Risk management is the prioritization of critical, sensitive, or valuable information technology assets in your enterprise, followed by assessment to identify vulnerabilities, estimation of the likelihood of any of those vulnerabilities being exploited by a threat actor, and the impact or consequence of that exploitation. Findings are addressed by accepting, avoiding, mitigating through controls, or transferring (insuring) identified risk.*

If your organization is not sure where to begin on a risk assessment, the U.S. Department of Homeland Security has created a Cybersecurity Evaluation Tool (CSET) to guide users through a step-by-step process to assess their cybersecurity readiness. Companies can download this free tool at https://ics-cert.us-cert.gov/Assessments. This is a non-technical assessment, predicated on responding to a series of questions regarding organizational processes.

6. MANAGE VENDORS AND CONTRACTORS

The process of procurement provides an opportunity to use market forces to affect security outcomes. Products should be demonstrably secure when purchased, and contractual agreements should address security updates, third-party testing requirements and other aspects of managing ongoing security. Further, organizations increasingly rely upon third parties to handle aspects of their information technology infrastructure, control systems and security. It is critical that these contractors, consultants and other third parties are appropriately managed with respect to monitored access, ethics and background.

Embedding cybersecurity in the procurement process is an important step for protecting critical systems and services. Including cybersecurity in the procurement process can ensure that those purchasing and supplying energy delivery systems consider cybersecurity starting from the design phase of system development. This further ensures that cybersecurity is implemented throughout the testing, manufacturing, delivery, installation and support phases of the product life cycle, improving overall reliability and reducing cybersecurity risks. DOE has created a guide that provides baseline cybersecurity procurement language for use by asset owners, operators, integrators and suppliers during the procurement process. This document can be found at:

http://connectedworld.com/wp-content/uploads/2014/08/Whitepaper_USDOE_CybersecurityProcurementLanguageForEnergyDelivery.pdf

Decades of familiarity with anti-virus programs have conditioned people to think of cybersecurity as a separate tool to be added on top of other products. Today's software and control systems should be developed and designed from the outset with security in mind. Network architecture and topology should minimize possible intrusions and allow a company to recognize when it is under attack.

- When possible, speak with vendors about the security characteristics of their products and incorporate cybersecurity as a key component in any new specifications your company develops.
- Use the power of the purse to require demonstrable security controls in products and services obtained through competitive procurement.

7. DETECT, RESPOND, AND RECOVER

Today, preventive controls such as firewalls, intrusion prevention systems, URL filtering, desktop anti-virus and email security have become less effective. Threat actors routinely use attacks that are not detected by perimeter or signature-based technologies, use encryption and obfuscation, and rely more on employee trustfulness than sophisticated attack methods. Your organization's ability to quickly detect and effectively respond to an intrusion is critical to limiting damage and loss. Note that these functions may be performed internally, or outsourced to a managed security service provider (MSSP).

Effective response can be performed through assigning responsibilities to existing operational roles. For example, help desk, desktop, server and network resources may all play a part in the identification, triage, investigation, confirmation and elevation of an observed event to incident status.

Containment, eradication and recovery of a confirmed compromise may be performed by removing the offending malware with tools, or by replacement and reimaging. Under some circumstances, and

depending on the role of the employee who normally uses the asset, digital media must be imaged for possible later forensic investigation, with chain-of-custody documentation to ensure defensibility in the event the information is used by law enforcement to charge an individual or organization with a crime.

Important questions should be asked after an incident that involves a key asset. Was the organization or individual targeted, or is this an unspecific campaign? What was the introduction vector of the compromise – email, removable drive, poisoned website – and has that introduction vector been locked down? For example, if the vector is a phishing message that leads to disclosure of credentials, all company email should be searched for other instances of the message to employees and removed.

Finally, communication is one of the most important aspects of incident response to manage. An errant public communication that personally identifiable information has been lost – prior to actually confirming that loss – can do much more harm than good. Further, sharing the information on a compromise – especially if determined to be targeted and focused on infrastructure or critical services – can help others to avoid loss as well. It is advisable to develop notification thresholds that, if met, would necessitate informing law enforcement, the federal government or regional emergency response.

A sample incident response plan and template documents for incident management may be found at http://www.sans.org/score/incident-forms//, and a contact list for sharing information is included as an appendix to this document.

Detect: Your company's ability to detect an intrusion is critical to a cybersecurity incident. To be able to detect, you need to develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

NIST suggests the Detect Function includes the following outcome categories: Anomalies and Events, Security Continuous Monitoring, and Detection Processes. The Detect function enables timely response and the potential to limit or contain the impact of potential cyber incidents.

Respond: As mentioned above, develop and implement the appropriate response activities, prioritized through the organization's risk management process (including effective planning), to take action regarding a detected cybersecurity event.

NIST suggests the Respond function includes the following outcome categories: Response Planning, Analysis, Mitigation, and Improvements. The Respond function is performed consistent with the business context and risk strategy defined in the Identify function. The activities in the Respond function support the ability to contain the impact of a potential cybersecurity event.

Recover: Once the incident is over, it is time to start your recovery process. To do this you need to develop and implement the appropriate activities, prioritized through the organization's risk management process, to restore the capabilities or critical infrastructure services that were impaired through a cybersecurity event.

NIST suggests the Recover function includes the following outcome categories: Recovery Planning, Improvements, and Communications. The activities performed in the Recover function are performed consistent with the business context and risk strategy defined in the Identify function. The activities in the Recover function support timely recovery to normal operations to reduce the impact from a cybersecurity event.

8. CONDUCT TRAINING AND EXERCISES

Training, assessment and system hardening are good, but they need to be practiced regularly in much the same way other physical and administrative security procedures are tested. In the same way utilities conduct exercises focused on physical security and disaster response, they should also focus upon cybersecurity scenarios. These exercises might range from sending a phishing email to employees to see if they click on the link to hiring a third party to attempt to penetrate your company's cyber defenses.

The Washington State Emergency Management Division recommends that information systems operators for critical infrastructure maintain a close and active relationship with their business continuity and disaster recovery personnel, as well as with local emergency managers. Developing these partnerships will enable a common understanding of vulnerabilities, and the integration of cybersecurity into existing training and exercise programs. For more information on cybersecurity and emergency management, please visit the following website.

http://mil.wa.gov/emergency-management-division/cyber-security-program

9. REPORT INCIDENTS

The best way to support your company's and your industry's cybersecurity defenses is to ensure that your company shares information on incidents in a timely manner through the appropriate channels.

Organizations should document their guidelines for interactions with local, state and federal organizations regarding incidents. While handling an incident, the organization will need to communicate with outside parties, such as other incident response teams, law enforcement, the media, vendors, and victim organizations. Because these communications often need to occur quickly, organizations should predetermine communication guidelines so that only the appropriate information is shared with the right parties.

It is important to share this information, so that regional and national events may be put into context in order to understand if an event may be in progress that is affecting more than a single organization. A disruption event may affect a geographical area, an infrastructure sector or the government, and it is not possible to know the scale of an event without appropriate information.

Sharing mechanisms are in place at the federal level through the Cyber Information Sharing and Collaboration Program (CISCP), which is an opt-in program operated through the National Cybersecurity and Communications Integration Center (NCCIC) and US-CERT.

Information sharing and analysis organizations (ISACs) exist for sharing incident and threat information possibly within your sector (water, energy, etc.). The purpose of an ISAC is for bi-directional information sharing. ISACs should inform members about threats seen elsewhere, and significant events should be shared with the ISAC with instructions on how the information may be further shared. ISACs are mainly free services, although some charge a membership fee.

Regionally, incident information may be shared through networks of trusted industry colleagues, or through organizations collaborate for this purpose. The Cyber Incident Response Collaboration and Analysis Sharing Organization (CIRCAS), the Agora (quarterly cybersecurity information sharing group), FBI InfraGard, and others facilitate this type of interaction in the state. See appendix B and C for listings of organizations.

Finally, if an incident is suspected as criminal, the FBI's cybercrime task force should be notified immediately.

10. ADDRESS PHYSICAL SECURITY OF CYBER ASSETS

Discussions of cybersecurity tend to focus upon firewalls, network infrastructure and control systems. It is important not to forget about protecting your company's physical assets as well. For example, if your company has a computer on its network in a remote location, ensure that access is controlled and monitored. Employees or contractors who log in to your system remotely may inadvertently compromise your security by misplacing their devices.

- Understand the physical attack vectors that exist into your network and restrict access to those points.
- Regularly review ingress/egress logs for spurious events such as access odd times of day.
- Regularly review camera/video data to identify suspicious precursory behavior such as individuals observing/photographing the data center.
- Ensure that generator fuel is not stored near the data center.
- Routinely inventory computing devices provided by the organization (especially mobile devices) to quickly identify lost or stolen assets.

11. CONCLUSION

These practices constitute a baseline for providing effective cybersecurity controls; they are not exhaustive or prescriptive, and are intended to help set direction for those organizations that need a starting point. Appendices to this document provide greater detail on cybersecurity focus areas, and if implemented, alignment with regulatory requirements and generally accepted standards of practice.

Cybersecurity resource issues in the public sector are a concern, and the reader is encouraged to investigate state initiatives that have been instantiated to address infrastructure protection and workforce development, and take advantage of emerging internship and apprentice programs.

APPENDIX A - UTILITY GUIDE

Washington State Electric Sector Cyber Guide

"We are continuing this policy in bleeding America to the point of bankruptcy." – Osama bin Laden

Smaller utilities may believe that they are "too small" or "no one would even be interested in them." The National Rural Electric Cooperative Association (NRECA) has stated that **"**Adversaries will go after the weakest link…" The majority of all utility companies have similar systems, regardless of size. For example, small distribution utilities have supervisory control and data acquisition (SCADA) systems which could be the same a large utility uses. Parties can penetrate and learn from smaller, less secure utilities to prepare an attack on a larger entity.

NIST FRAMEWORK: IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

The federal cybersecurity framework was developed by NIST at the direction of the President through Executive Order 13636. The framework is a distillation and repackaging of several authoritative standards of practice, including the NIST 800-53 standard, the International Standards Organization (ISO) 27001/27002, and others. Implementing the framework is voluntary, and can be performed by any size organization; the implementation specifics are different for organizations of varying maturity in the application of cybersecurity policies, technical controls and processes.

This part of the guide is written as a primer to assist electric utilities (generation, transmission, distribution) in establishing the management of activities around cybersecurity, and using the language embedded in the framework for consistency. This guide is not a substitute for the actual implementation of the framework itself, but rather a primer on the various issues that must be addressed to identify, protect, detect, respond to and recover from cyber attacks, and ensure that real damage to operations and finances is minimized.

***IDENTIFY** the **risk** environment – **assets** that may be stolen or disrupted to cause financial loss or service disruption, as well as the **threats** that would be motivated by attempting to cause that loss or disruption, and the **consequence** of those threats being realized. Assigning dollar values to those potential impacts will be useful in determining the level of investment that is applicable to mitigating the risks, as well as prioritizing those mitigation activities.*

---

1) Create an inventory of your critical IT assets, keeping in mind what is critical to providing service as well as keeping the business operating. Examples of critical assets are the information technologies that support:
    a. Generating resources
    b. Water systems
    c. Transmission and distribution facilities
    d. Control systems
    e. Regulated records (Personally Identifiable Information (PII), Protected Health Information (PHI), Personally Identifiable Financial Information (PIFI))
    f. Other sensitive information (operational details that disclose vulnerabilities)

2) Threats to those assets:
    a. Unauthorized disclosure
    b. Theft of funds
    c. Service disruption
    d. Fines, regulatory oversight, and other consequential impacts
3) Impacts if those threats are realized:
    a. Loss of life; cascading failure to other services or infrastructure
    b. Loss of operating funds
    c. Cost of compliance with records breach reporting statute
    d. Fines by federal regulators, increased regulatory oversight, loss of ability to handle credit card information, other ancillary impacts

---

PROTECT *what is important; ensure that the critical assets identified have appropriate preventive controls in place to protect against the threats previously identified, and processes to ensure that non-technical aspects of protection are addressed.*

---

1) Develop governance and policy
    a. Business-unit, IT management, and executive leadership team for security governance (for example, development and implementation of policy, budget approval, etc.)
    b. Organization-wide security policy
    c. Specific policies regarding acceptable use of organizational technology, procurement requirements for security, non-disclosure of sensitive materials, etc.
    d. Response and recovery planning
2) Evaluate security operations framework
    a. Operational elements you **should** have in place (the NIST framework can guide this)
    b. Identify what you have in place now
    c. The gap between as-is and desired state
3) Protective/preventive controls. These include processes for reducing the "threat surface" of critical assets, requirements that are applied to vendors, service providers and other third parties, policy-based controls that are not enforced with technology, and those that are. A non-exhaustive list of examples:
    a. Strong authentication mechanisms
    b. Vulnerability identification and management (keeping software patched/updated)
    c. Desktop anti-virus (aka end-point protection)
    d. Email security – filtering hostile links and attachments
    e. URL filtering for web traffic
    f. Separation of sensitive operations and personal use of technology
    g. Third-party management
    h. Network access controls (firewalls, segmentation, use of VLANs)
    i. Employee education and awareness
4) Routinely conduct assessments to identify vulnerabilities. Each vulnerability identified should have a plan to remediate, and the plan prioritized by severity and potential for exploit.
    a. Conducted internally, using commercial tools
    b. Conducted by a commercial third-party
    c. Conducted by a peer organization
    d. Conducted by DHS or another federal entity

DETECT *events that indicate compromise of assets, and actively seek out information on current threats. Preventive controls will fail against a highly-resourced threat actor such as rogue nation-states, terrorists, and organized crime, and detection, combined with rapid response, is an exceptional compensating control.*

1) Collect information on current threats. This will allow for the detection of specific indicators of compromise, which may be associated with targeted attempts at disruption or destruction.
    a. ES-ISAC
    b. US-CERT
    c. Distribution products from Fusion Center, law enforcement, etc.
    d. Open-source intelligence
2) Continuously monitor networks and key assets for suspicious events, trends or traffic
    a. Conducted internally, using commercial SIEM products
    b. Commercial monitoring and alerting services
    c. Non-profit services developed with government funding
    d. Electric-sector-specific services
3) Detection process
    a. Review your logs
    b. Conduct automated event aggregation and correlation

RESPOND – *Develop methods to rapidly address attacks in progress, and minimize the residence time of compromised assets in the environment*

1) Response planning
    a. Create a cyber incident response plan
    b. Integrate with your emergency response plan
    c. Integrate with your local emergency management organization
    d. Exercise the plan
2) Communications
    a. Within the organization
        (1) To other entities: Notify Electricity Sector Information Sharing and Analysis Center (ES-ISAC)
        (2) NERC
        (3) If criminal activity is suspected, notify law enforcement
        (4) If operations are significantly impacted, notify your local emergency operations center
        (5) Inform customers if and when appropriate
3) Analysis
    a. Determine the system compromise/intrusion (e.g. user compromise, root compromise, malicious code, etc.)
    b. Describe the impact of the cyber incident
    c. Consider engaging with outside resources
    d. Begin recovery planning
4) Mitigation

a. Isolate and contain compromised assets
b. Apply corrective action to remove the compromise; confirm effectiveness.
c. Conduct further communications

5) Improvements
    a. Developafter action report
    b. Update incident response plan
6) Conduct exercises to evaluate the efficacy of response planning, identify necessary improvements, and meet key response objectives
    a. Tabletop
    b. Functional

RECOVER – *Bring supporting technology back to operational state and ensure that security issues have been resolved*

---

1) Recovery planning
    a. Create a compromised asset recovery plan
    b. Integrate with your emergency response plan
    c. Exercise the plan
3) Execute recovery plan
    a. Perform testing to ensure that compromised assets have been repaired
    b. Return the asset into service
    c. Continue to monitor network communications for that asset for a period of time
4) Execute continuous process improvements
    a. Conduct an objective after-action review of the recovery process
    b. Identify and enact changes to process to improve the efficiciency of the recovery process
5) Conduct additional communication – See paragraph “Respond”, section 2 above

STEPS FOR UTILITIES TO TAKE TO DEVELOP A RISK PLAN

"The ongoing assessment of security threats, balanced against the existence and adequacy of security controls at your organization is needed to ensure that security controls and countermeasures in place are commensurate with potential risks. The effort is never ending." NRECA's *Guide to Developing a Cyber Security and Risk Mitigation Plan – Update 1*.

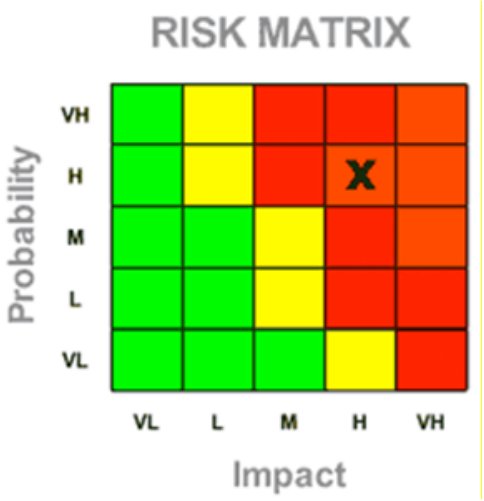
- Develop a cybersecurity policy tailored to your utility. Without it you have no baseline for the program.
- Develop a list of cybersecurity risks for your utility.
- Develop a cybersecurity strategy to assess, prioritize and manage your risk. Here are some steps to follow.

Step 1: Rank the major threat categories. Example of threats to include:

Threat category	Risk Description
Sensitive Data Loss	Lack of breach policy (in work), lack of breach education for employees (only HIPAA in place for ER), communication plan not documented, management response not documented
Unsupported OS and applications	Windows XP End of Life (EOL), Windows Server 2003 EOL, AIX EOL, software EOL (e.g., PassPort), vulnerabilities in non-supported software, vulnerabilities in unsupported browser plug-ins, dependence on legacy software (Java)
Denial of Service	Lack of detective capabilities, lack of ISP Service Level Agreement (SLA), lack of annual exercise, lack of mitigation contract
Policy Non-Compliance	No annual review of accounts, use of non-admin accounts for server admin functions, disabled accounts not deleted, account termination not timely, application access management inconsistent, access for OT systems not centralized, least privilege not enforced, roles not defined for Role Based Access Control, system use notification missing from systems, control of remote access for employees/vendors inconsistent, sensitive information not identified and/or controlled, audit records (logs) not managed, lack of log analysis, lack of log processing alerts, unknown log security, lack of targeted cybersecurity training, inconsistent user IDs, no centralized access control of non-windows systems, media sanitization inconsistent, lack of approval of maintenance tools for IT systems, lack of audit capability, lack of policy enforcement capability, no documented risk ITS assessment, no integration with District risk management process
Application Security Risks	Applications with non-standard authentication/authorization controls are not managed centrally, vulnerabilities for non-standard systems or systems out of IT control are not known or applied using IT standard
Third-Party Relationship Risks	Vendor supplied software, vendor managed support, vendor managed maintenance, vendor maintenance tools
Operational Security Risks	Recovery from malware, recovery from data loss, security breach, hardware failure, backup/restore failure, employee actions (delete or destroy data or software) intentional or unintentional (insider threat)
Physical Security Risks	Physical access to data center unauthorized, access to data center not possible, failure of UPS, failure of fire control system, physical disaster recovery planning not integrated with ITS DRP, no EOC standup processes for IT
Business Risks	Inconsistent update process for BCP, lack of integration of BCP and DRP, business IT risks unknown, no annual analysis of DRP business critical applications, no identification of sensitive information within DRP (segregation issue)

Access Management	Lack of District unified process (physical-ER-IT), lack of administrative user access control, lack of OS authentication integration, lack of application integration, no identity and access management solution, lack of management accountability, inconsistent or missing role based access control, default or vendor set credentials are not always reset, systems use notification not consistent in all District systems, shared user accounts not managed consistently
Malware	Uncontrolled infections, unknown exploits, unsupported software, unknown software, loss of data, IE, loss of sensitive info, loss of critical business data, lack of detective capability, lack of detection and eradication capability, Web Mail

Step 2: Identification of the risks that were created by the selected threat. An example would be the threat "malware" has a risk identified as uncontrolled infections (viruses, Trojans, worms and key loggers). Another risk identified under the threat "malware" was lack of detective capability (lack of anti-virus effectiveness, late patching of 0-day vulnerabilities, and lack of identification of current "in the wild" exploits).



The risks associated with a threat are detailed within the Risk Registry (as shown in the table above) and should be updated as the threats and risks evolve.

Step 3: Determine how to lower the risk of the threat.

1. Develop an incident response plan so you stop the "hair on fire" response. Should be in coordination with local, state and federal authorities.
2. Continuous monitoring of the risks by utilizing any of the following:
   - DHS groups such as InfraGard (FBI), ICS-CERT or DHS HSIN
   - Local groups like CIRCAS or AGORA
   - Situational awareness for your specific industry/sector from the ISAC (Information Sharing and Analysis Center)
     - These ISACs are available to the financial sector (FS-ISAC), energy sector (ES-ISAC), multi-state sector (MS-ISAC), etc.
   - International organizations like ISC2, ISACA and SANS for free resources.
   - Networking among peers.
   - Developing internal training.
   - Coordinating with local and state officials on Cybersecurity Emergency Response plan.

REFERENCES and RESOURCES FOR UTILITIES:

- From the *Roadmap to Achieve Energy Delivery Systems Cybersecurity (2011) accessible at: http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf*:
    - *Build a Culture of Security.* Through extensive training, education and communication, cybersecurity "best practices" are encouraged to be reflexive and expected among all stakeholders.
    - *Assess and Monitor Risk*. Develop tools to assist stakeholders in assessing their security posture to enable them to accelerate their ability to mitigate potential risks.
    - *Develop and Implement New Protective Measures to Reduce Risk*. Through rigorous research, development and testing, system vulnerabilities are revealed and mitigation options are identified which has led to hardened control systems.
    - *Manage Incidents*. Facilitate tools for stakeholders to improve cyber intrusion detection, remediation, recovery and restoration capabilities.
    - *Sustain Security Improvements*. Through active partnerships, stakeholders are engaged and collaborative efforts and critical security information sharing is occurring.
- The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) – model allows companies to evaluate, prioritize and improve cybersecurity activities by allowing them to make comparisons between their activities and industry-vetted practices. Available at: http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity.
- Risk Management Process (RMP) Guideline Final (May 2012) – The RMP is intended to enable participants in the electric power sector to apply effective cybersecurity risk-management processes that can be tailored to an individual organization's needs. Available at: http://energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012.
- DOE's Cybersecurity Procurement Language for Energy Delivery Systems – Energy delivery systems, which are used to monitor and control the production, transfer and distribution of energy, are critical to the effective and reliable operation of North America's energy infrastructure. Our 21st century way of life is made possible by the vast network of processes enabled by these systems, as well as the interconnected electronic components, communication devices, and people who monitor and control those processes. Available at: http://www.energy.gov/oe/downloads/cybersecurity-procurement-language-energy-delivery-april-2014.

  Cybersecurity threats, whether malicious or unintentional, pose a serious and ongoing challenge for the energy sector. Embedding cybersecurity in the procurement of energy delivery systems is an important step for protecting these systems from cybersecurity threats. Including cybersecurity in the procurement process can ensure that those purchasing and supplying energy delivery systems consider cybersecurity starting from the design phase of system development. This further ensures that cybersecurity is implemented throughout the testing, manufacturing, delivery, installation and support phases of the product life cycle, improving overall reliability and reducing cybersecurity risks.

To assist with embedding cybersecurity in the procurement of energy delivery systems, this Cybersecurity Procurement Language for Energy Delivery Systems guidance document provides baseline cybersecurity procurement language for use by asset owners, operators, integrators and suppliers during the procurement process.

- The Cybersecurity Risk Information Sharing Program (CRISP) is a public-private partnership to facilitate the timely sharing of cyber threat information and develop situational awareness tools to better protect against and respond to cybersecurity threats. The capability enhances the energy sector's ability to identify, prioritize and coordinate the protection of critical infrastructure and key resources, reducing the risk of energy disruptions due to cyber events. CRISP uses technical expertise and technologies developed at the Pacific Northwest National Laboratory (PNNL) and machine speed information sharing technologies developed by Argonne National Laboratory, leverages access to government cybersecurity information, and collaborates with industry subject matter experts at the North American Electric Reliability Corporation's (NERC) Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Please contact the Electricity Sector Information Sharing and Analysis Center for additional information.

  NERC CIP Standards 002–009 – NERC critical infrastructure protection (CIP) standards for entities responsible for the availability and reliability of the bulk electric system. Available at: http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. Note: you must have an account with NERC to access these.

- Electricity Sector Information Sharing and Analysis Center (ES-ISAC) – The ES-ISAC establishes situational awareness, incident management, and coordination and communication capabilities with the electricity sector through timely, reliable and secure information exchange. The ES-ISAC shares critical information with electric industry participants regarding infrastructure protection. The goal is to promptly disseminate threat indications, analyses and warnings and issue alerts to assist electricity sector participants in taking protective action. In addition to its information sharing and coordination roles, the ES-ISAC's other responsibilities include analyzing event data, working with the ISACs for other critical infrastructure sectors to exchange information and assistance, performing cyber risk assessments, and participating in critical infrastructure exercises and industry outreach. Their website is: https://www.esisac.com/SitePages/Home.aspx.

- The Energy Sector Security Consortium, Inc. (EnergySec) is a United States 501(c)(3) non-profit organization formed to support organizations within the energy sector in securing their critical technology infrastructures. EnergySec supports collaborative programs and projects with the mission of strengthening the cybersecurity posture of critical energy infrastructures. Their website is: http://www.energysec.org/

- NIST IR 7628: Smart grid cybersecurity strategy and requirements. Available at: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

- NIST SP800-53, Recommended Security Controls for Federal Information Systems and Organizations: Catalog of security controls in 18 categories, along with profiles for low-, moderate- and high-impact systems. Available at: http://csrc.nist.gov/publications/PubsSPs.html.

- NIST SP800-82, DRAFT Guide to Industrial Control Systems (ICS) Security. Available at: http://csrc.nist.gov/publications/PubsSPs.html.

- NIST SP800-39, DRAFT Integrated Enterprise-Wide Risk Management: Organization, mission, and information system view. Available at: http://csrc.nist.gov/publications/PubsSPs.html.
- AMI System Security Requirements: Security requirements for advanced metering infrastructure. Available at: http://energy.gov/oe/downloads/ami-system-security-requirements-v101-1.
- ISO/IEC (International Organization for Standardization) 27001, Information Security Management Systems: Guidance on establishing governance and control over security activities (this document must be purchased, a preview is available: http://www.iso.org/iso/home/store/publication_item.htm?pid=PUB200004).
- IEEE (Institute of Electrical and Electronics Engineers) 1686-2007, Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities (this document must be purchased, preview available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4453853&queryText%3DStandard+for+Substation+Intelligent+Electronic+Devices).
- NIST's Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 2014, available at: http://www.nist.gov/cyberframework/.

APPENDIX B - STATE CYBER RESOURCES

Agora

The Agora is a quarterly meeting that has been ongoing for more than 18 years. Established and conducted by Kirk Bailey, CISO of the University of Washington, the Agora brings together information security practitioners, executives, government and military, entrepreneurs, vendors and consultants for networking, information-sharing, and 3-4 presentations by subject matter experts.

The Agora may not be attended without membership, as it is a network of trust. In order to be considered for membership, send a request to agora@anetworkoftrust.org.

CIRCAS

Cyber Incident Response Coalition for Analysis Services (CIRCAS) – CIRCAS is a regional organization 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. You must be nominated by a CIRCAS member to participate. If interested, contact the state emergency management division cyber security manager (www.mil.wa.gov).

WASHINGTON STATE EMERGENCY MANAGEMENT DIVISION CYBERSECURITY PROGRAM

For the last several years, the Washington State Military Department has worked aggressively to prepare the state for cyber emergencies. Extensive outreach and program development efforts by the National Guard and other state agencies culminated in the creation of a Cybersecurity Program within the Emergency Management Division. The manager of the program functions as the state's cybersecurity policy leader and strategist for regional significant cyber incident response. The goal of the program is to fully integrate cybersecurity into all phases of statewide emergency management and to promote community cybersecurity for public safety and resiliency of commerce. Available at: http://mil.wa.gov/emergency-management-division/cyber-security-program

FEDERAL BUREAU OF INVESTIGATION

The Federal Bureau of Investigation (FBI) has a cyber task force and hosts the Washington State Fusion Center. The FBI may be able to assist critical infrastructure owner/operators when there is a cyber-attack or suspected cyber incident. The FBI encourages reporting of suspected cyber-attacks by critical infrastructure owners.

The Seattle Office number is (206) 622-0460 or email Seattle.fbi@ic.fbi.gov.

NATIONAL GUARD

Under certain circumstances, the National Guard may be called upon to conduct a risk assessment of critical infrastructure, to include energy, dams, water, and government facilities sectors.

WA State CIO

The Chief Information Officer sets information technology (IT) policy and direction for the State of Washington's agencies, boards and commissions. Main website: www.watech.wa.gov

PUBLIC REGIONAL INFORMATION SECURITY EVENT MONITORING (PRISEM) PROJECT

PRISEM monitors cybersecurity for local governments, maritime ports and energy sector in the Puget Sound metropolitan area and is attempting to expand statewide. PRISEM 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, PRISEM can help supply situational awareness regarding the threat surface of a region, and provide a common operating picture across the participating organizations.

WASHINGTON CYBER INCIDENT RESPONSE CENTER (WACIRC)

The WACIRC was instituted by Washington state with the goal of proactively addressing the threats posed to our citizens from criminal and terrorist acts by sharing information with public- and private-sector organizations around the state. The service is free of charge; more information at: www.watech.wa.gov.

WASHINGTON STATE FUSION CENTER

The WSFC monitors alerts from the PRISEM system, as well as reports of activity and incidents that are reported through the suspicious activity reporting (SAR) intake address. With access to federal systems, law enforcement, the Department of Homeland Security, and with a range of information sharing and response capabilities, WSFC provides be-on-the-lookout (BOLO) alerts, analysis products, and can escalate events into federal visibility when needed. If you want to receive Cyber Situational Awareness Bulletins and BOLOs from the WSFC, send your full name, agency, title/position, and official email to intake@wsfc.wa.gov. Also report a suspicious event by emailing intake@wsfc.wa.gov. Main website: http://wsfc.wa.gov/.

WASHINGTON UTILITIES and TRANSPORTATION COMMISSION

The Washington Utilities and Transportation Commission (UTC) is a three-member commission appointed by the governor and confirmed by the state Senate. Main website: http://www.utc.wa.gov/Pages/default.aspx. The UTC brings together providers of critical infrastructure for workshops and focus groups, and to foster dialog between utility providers and regulators around issues of cybersecurity, as well as other issues.

APPENDIX C - FEDERAL CYBER RESOURCES

CYBER RESILIENCE REVIEW (CRR)

The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of 10 domains including risk management, incident management, service continuity and others. The assessment is designed to measure existing organizational resilience as well as provide a gap analysis for improvement based on recognized best practices.

CYBER SECURITY EVALUATION TOOL (CSET)

The Cyber Security Evaluation Tool (CSET®) is a Department of Homeland Security (DHS) product that assists organizations in protecting their key national cyber assets. It was developed under the direction of the DHS Industrial Control System Cyber Emergency Response Team (ICS-CERT) by cybersecurity experts and with assistance from the National Institute of Standards and Technology (NIST). This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.

DEPARTMENT OF HOMELAND SECURITY (DHS)

The Office of Cybersecurity and Communications (CS&C) works with state and local government as well as private sector partners to minimize the impact of cybersecurity incidents. Two of CS&C's National Cybersecurity and Communications Integration Center components, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and United States Computer Emergency Readiness Team (US-CERT) work to mitigate cybersecurity incidents in close coordination with public and private sector partners.

ICS-CERT provides onsite support to owners and operators of critical infrastructure, including incident response, forensic analysis and site assessments. ICS-CERT also provides tools and training designed to increase stakeholder awareness of the threats posed to industrial control systems.

The ICS-CERT website provides various resources for owners and operators of critical infrastructure and the industrial control systems that operate many of the key functions of their facilities, such as the SCADA system. The website contains links to resources such as alerts, advisories, newsletters, training and recommended practices, as well as a large list of standards and references.

The ICS-CERT website can be found here: https://ics-cert.us-cert.gov/. ICS cyber incidents can be reported to: ics-cert@hq.dhs.gov.

DEPARTMENT OF HOMELAND SECURITY PROTECTIVE SECURITY ADVISORS AND CYBER SECURITY ADVISORS

The Department of Homeland Security (DHS) Protective Security Advisor (PSA) program offers critical infrastructure owner/operators a conduit to many free services such as security training, site assessments and assistance with local exercise coordination. Washington state's PSA is Dave Holcomb (david.holcomb@hq.dhs.gov).

There is also a regionally based Cyber Security Advisor (CSA) that functions in the same capacity for cybersecurity-specific issues. Washington's CSA is based in San Francisco, CA (Deron Mcelroy, deron.t.mcelroy@hq.dhs.gov).

More information on the PSA program may be found here: http://www.dhs.gov/protective-security-advisors.

iGUARDIAN

The FBI recently released the iGuardian portal as a pilot program designed to give companies a designated location to report cyber threats they've encountered. Initially, the program will be open only to members of the InfraGard Network (see above). The iGuardian portal offers a one-stop-shop for cyber incident reporting. Reports received by iGuardian will go to the local FBI office and the FBI may follow up with the reporting entity. More information on becoming an InfraGard member can be found here: www.infragard.org/.

THE INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM (ICS-CERT)

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among federal, state, local and tribal governments and control systems owners, operators and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures.

Complete list of DHS resources at www.dhs.gov/sites/default/files/publications/Policy-PSO/private_sector_resource_catalog_December_2012.pdf

INFRAGARD

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal and security matters. InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector.

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes. Membership is free and open to all critical infrastructure owners and operators.

More information, including information on membership, can be found here: www.infragard.org/.

INFORMATION SHARING AND ANALYSIS CENTERS (ISACs)

The mission of the National Council of ISACs (NCI) is to advance the physical and cybersecurity of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government. Members of the Council are the

individual Information Sharing and Analysis Centers (ISAC) that represent their respective sectors. Main website: www.isaccouncil.org.

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER (NCCIC)

The NCCIC, within the Office of Cybersecurity and Communications, serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated. NCCIC partners include all federal departments and agencies; state, local, tribal and territorial governments; the private sector; and international entities. The center's activities include providing greater understanding of cybersecurity and communications situation awareness vulnerabilities, intrusions, incidents, mitigation and recovery actions. Main website: www.dhs.gov/about-national-cybersecurity-communications-integration-center.

Cyber incidents can be reported to the NCCIC watch desk at: NCCIC_ WatchandWarning@hq.dhs.gov.

REGIONAL RESILIENCY ASSESSMENT PROGRAM (RRAP)

The RRAP evaluates critical infrastructure on a regional level to examine vulnerabilities, threats and potential consequences from an all-hazards perspective, identifying dependencies, interdependencies, cascading effects, resilience characteristics and gaps. Each year, the Department selects RRAP projects with input and guidance from federal and state partners. RRAP projects, which are voluntary and non-regulatory, focus on specific infrastructure sectors within geographic areas and address a range of hazards that may have significant regional and national consequences.

SANS

The Twenty Critical Security Controls have already begun to transform security in government agencies and other large enterprises by focusing their spending on the key controls that block known attacks and find the ones that get through. Agreed upon by a powerful consortium which included NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities, the automation of these top 20 controls will radically lower the cost of security while improving its effectiveness.

APPENDIX D - GLOSSARY AND ACRONYMS

GLOSSARY

Category	The subdivision of a Function into groups of cybersecurity outcomes, closely tied to programmatic needs and particular activities. Examples of Categories include “Asset Management,” “Access Control,” and “Detection Processes.”
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on cybersecurity, national economic security, national public health or safety, or any combination of those matters.
Cybersecurity	The process of protecting information by preventing, detecting, and responding to attacks.
Cybersecurity Event	A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation).
Detect (function)	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Framework	A risk-based approach to reducing cybersecurity risk composed of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. Also known as the “Cybersecurity Framework.”
Framework Core	A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core comprises four types of elements: Functions, Categories, Subcategories, and Informative References.
Framework Implementation Tier	A lens through which to view the characteristics of an organization’s approach to risk—how an organization views cybersecurity risk and the processes in place to manage that risk.
Framework Profile	A representation of the outcomes that a particular system or organization has selected from the Framework Categories and Subcategories.
Function	One of the main components of the Framework. Functions provide the highest level of structure for organizing basic cybersecurity activities into Categories and Subcategories. The five functions are Identify,
Identify (function)	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Informative Reference	A specific section of standards, guidelines, and practices common among critical infrastructure sectors that illustrates a method to achieve the outcomes associated with each Subcategory.
Mobile Code	A program (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics.
Protect (function)	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
Privileged User	A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Recover (function)	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
Respond (function)	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (a) the adverse impacts that would arise if the circumstance or event occurs; and (b) the likelihood of occurrence.
Risk Management	The process of identifying, assessing, and responding to risk.
Subcategory	The subdivision of a Category into specific outcomes of technical and/or management activities. Examples of Subcategories include “External information systems are catalogued,” “Data-at-rest is protected,” and “Notifications from detection systems are investigated.”

ACRONYMS

CCS	Council on Cyber Security
COBIT	Control Objectives for Information and Related Technology
CRISP	Cybersecurity Risk Information Sharing Program
DCS	Distributed Control System
DHS	Department of Homeland Security
ESCC	Electricity Subsector Coordinating Council
EO	Executive Order
FBI	Federal Bureau of Investigation
HSIN	Homeland Security Information Network
ICS	Industrial Control Systems
IEC	International Electro technical Commission
IR	Interagency Report
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISACA	Information Systems Audit and Control Association
ISC2	International Information Systems Security Certification Consortium (ISC)^2
ISO	International Organization for Standardization
IT	Information Technology
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRECA	National Rural Electric Cooperative Association
PRISEM	Public Regional Information Security Event Monitoring
RFI	Request for Information
RMP	Risk Management Process
SANS	The SANS Institute
SCADA	Supervisory Control and Data Acquisition
SIEM	Security information and event management
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team