DRAFT

HOMELAND SECURITY REGION 5

CYBERSECURITY RESILIENCE CONOPS (DRAFT v3)

Table of contents

1.0 INTRODUCTION 2
1.1 Purpose 2
1.2 Background 2
1.3 Scope 2
1.4 Objectives 2
2.0 Current Options and Processes for Reporting 3
2.1 Single Point of Contact Reporting at the State and Local Level 3
2.2 Department of Homeland Security and Federal Law Enforcement 3
2.3 Washington State Fusion Center 3
3.0 Local and Statewide Reporting Operations 4
3.1 OVERVIEW 4
3.2 CATEGORIES 4
3.3 INCIDENT REPORTING – Situational Awareness 5
4.0 Submission, Analysis, and Dissemination 6
4.1 Analysis of Agency Incident/Event Data 6
4.2 Severity Rating 7
4.3 Cyber Insider Alert and Notification Publications 7
4.3.2 WSFC Products Related to Cyber Incident Response 8
4.4 Onsite Incident Response to Agencies 8
4.5 Incident Escalation 10
4.6 Notification of Other Related Organizations, Emergency Management, and Law Enforcement 10
4.7 Communications 10
4.7.1 Communication Guidelines 11
4.8 Regulatory Requirements 11
5.0 Securing and Safeguarding Information 11
5.1 Confidentiality 11
5.2 Outreach and Education 11
Appendix A Regulatory Requirements 12
Appendix B Washington State Fusion Center Suspicious Activity Report 14
Appendix C DOJ CTF Compromised Computer Network Incident Worksheet 20
Appendix D Traffic Light Protocol 24
Appendix E Federal Points of Contact 25
Appendix F List of Acronyms 27
Appendix G Cyber Security Glossary to include Common Threat Vectors 29
Appendix H Cybersecurity Doctrine and Resources 36
Appendix I Cyber Resource Compendium 40
Appendix J Cybersecurity Training 46

1.0 INTRODUCTION

1.1 Purpose

The Region 5 Cyber Resiliency Concept of Operations (CONOPS) enables information sharing and analysis that can assist state, local, and tribal agencies, the public and private sector, critical infrastructure providers, and key resource stakeholder organizations in the performance of their public safety, security, continuity, and disaster resilience responsibilities. This CONOPS focuses on cybersecurity incident reporting and response in Region 5 – Pierce County. It suggests processes, protocols, and policies that any stakeholder organization can put into practice to increase their resilience and response capabilities before, during, and after a significant cybersecurity incident. It includes suggestions for tools and specific guidelines by which an organization will be able to better detect, triage, and respond effectively to a cybersecurity intrusion or compromise. It specifically includes guidance for engaging with the local cyber community including public and private sector partners, law enforcement, and State and Federal resources.

1.2 Background

Stakeholders consistently identified a gap in cyber reporting capabilities and recommended a process compatible across the region. This effort falls in line with 2013 and 2016 presidential directives on information sharing:

2013 Presidential Policy Directive 21 (PPD-21)

2016 Presidential Policy Directive 41 (PPD-41)

1.3 Scope

This CONOPS is designed to address the needs of all organizations—public, private, academic, and healthcare—in Pierce County. As this includes critical infrastructure and key resources (CIKR), it will include specific references to regulatory and best practice guidance toward response notification and resource and information sharing within the cyber community of Pierce County and its dependent neighbors. This document supports and does not supplant existing cyber-related local, state, or federal plans, policies, directives or executive orders. It is not intended to be a tactical or operational plan for responding to cyber incidents. Rather, it establishes coordination and cooperative mechanisms, and a framework to facilitate the development of collaborative or agency-, organization-, or sector-specific prevention, protection, mitigation, response, and recovery actions and plans.

1.4 Objectives

- **Create a working Concept of Operations to which organizations can and will turn to for guidance on when, how, and whom to notify during a significant cyber incident.**
- **Provide specific contact(s) for reporting significant cyber incidents.**
- **Provide information and analysis, advisories, and two-way cross-sector information support to cyber preparation, planning, and response and recovery efforts.**
- **Encourage notification and information sharing across sectors and jurisdictions**

2.0 CURRENT OPTIONS AND PROCESSES FOR REPORTING

2.1 Single Point of Contact Reporting at the Federal, State, and Local Level

Currently several federal agencies collect significant cyber incident reports through different portals or websites. However, in the words of the National Cybersecurity and Communications Integration Center (NCCIC), "a report to one is a report to all." Meaning when an incident or threat is reported to a federal or state agency, that agency then has the responsibility to report-out to other federal or state counterparts that the incident or threat may affect or be affected by.

Often agencies have a regulatory requirement to report to federal partners and must follow strict protocols. We encourage agencies to work with federal, state, and local partners to ensure information is disseminated and shared at all levels. Organizations who do have a regulatory requirement to report to a federal agency are encouraged to utilize the both the Washington State Fusion Center's (WSFC) reporting portals, email, or phone number to report cyber threats and disruptions, as well as 'cc' the South Sound Regional Intelligence Group (SSRIG) for Pierce County. Likewise, the regional DHS Cybersecurity Advisor (CSA) will serve as a valuable advisor on potential resources or assistance available to organizations.

The following are the partners collecting reports on significant cyber events.

2.2 Department of Homeland Security and Federal Law Enforcement

The DHS NCCIC has a wide variety of resources available to assist organizations with their cyber risk assessments, penetration testing, as well as procedure and policy development, following the NIST 800-53 guidance. DHS encourages organizations to report incidents, especially if they affect critical infrastructure or security. Similarly, the FBI has online tools for reporting cyber incidents and encourages anyone to report using those tools. The local offices of the US Secret Service participate in an Electronic Crimes Task Force which specifically will work with organizations that have suffered a financial loss or crime. Contact information for these organizations are included in **Appendix E**.

2.3 Washington State Fusion Center

The Washington State Fusion Center (WSFC) is a clearinghouse for local, State, Federal, Tribal and Territorial law enforcement information and Intelligence gathering organizations. WSFC collects, writes, and disseminates raw reporting, produces cyber analysis based upon raw reporting and other local and national sources and analysts have sufficient cyber knowledge to receive, relay, and analyze cyber incidents and reporting. Ideally, they will be able to provide input information about the incident, and referral to the appropriate or required organizational and assistance resources. These might include law enforcement, DHS, NCCIC, Washington State Emergency Management Division (EMD), Cyber Incident Response Coalition & Analysis Sharing (CIRCAS), the National Cyber Forensics & Training Alliance (NCFTA), and or other community resources. WSFC will directly communicate to the reporting agency as well as all affected agencies to provide a status update and suggested mitigation or response activities. Currently the WSFC is not a 24-7 center.

2.4 Local Law Enforcement and Intelligence – South Sound Regional Intelligence Group

The SSRIG is a clearinghouse for local law enforcement information and intelligence gathering across Pierce County. SSRIG collects, analyzes, and disseminates raw reporting, and produces

analysis based on local raw reporting and other regional and national reporting. SSRIG is a conduit to and from the WSFC specific to the Pierce County region.

3.0 LOCAL AND STATEWIDE REPORTING OPERATIONS

3.1 OVERVIEW

It is the responsibility of any organization to combine the highest qualified and trained cybersecurity professionals, processes, and technology to produce a sufficient level of technological expertise to accurately and efficiently analyze new or evolving security events. The success or failure of cyber response operations depends significantly on how accurate an organization's security analysts judge the severity as security incidents emerge.

3.2 CATEGORIES

A computer incident may be defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. To clearly communicate incidents and observable occurrences in a network or system it is necessary for an organizational incident response teams to adopt a common set of terms and relationships between those terms. The following table outlines categories of incidents or events as suggested by NIST in its Special Publication 800-61.

Table 3-1 Incident Categories
***Defined by NIST Special Publication 800-61**

CATEGORY	NAME	DESCRIPTION	REPORTING TIMEFRAME
CAT 0	**Exercise/Network Defense Testing**	This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses.	Not Applicable; this category is for each agency's internal use during exercises.
CAT 1	***Unauthorized Access**	In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource	Within one (1) hour of discovery/detection.
CAT 2	***Denial of Service (DoS)**	An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.	Within two (2) hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity.
CAT 3	***Malicious Code**	*Successful* installation of malicious software (i.e. virus, worm, Trojan horse, or other code-based malicious entity that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.	Daily Note: Within one (1) hour of discovery/detection *if* widespread across agency.
CAT 4	***Improper Usage**	A person violates acceptable computing use policies	Weekly

Table 3-2 Federal Agency Event Categories

CATEGORY	NAME	DESCRIPTION	REPORTING TIMEFRAME
CAT 5	**Scans/Probes/Attempted Access**	This category includes an activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service.	Monthly Note: If system is classified, report within one (1) hour of discovery.
CAT 6	**Investigation**	*Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.	Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated.

3.3 INCIDENT REPORTING – SITUATIONAL AWARENESS

Reports shall be transmitted in a manner consistent with their sensitivity, severity, and needed resources. Reporting should not be delayed to gain additional information. The WSFC will anonymize all information used for generating reports. Reports can be submitted to the via the following methods:

EMAIL	intake@wsfc.wa.gov	PCINTEL@piercecountywa.gov	soc@msisac.org
PHONE	206.262.2285	253-573-2434	1-866-787-4722
HOTLINE	1.877.843.9522		
FAX	206.224.5454		
Fusion Center SAR	http://www.wsfc.wa.gov/Report		

Due to public disclosure laws, place a phone call to relay any specific sensitive information. The WSFC will alternatively utilize the Homeland Security Information Network (HSIN) to further protect conversation details from disclosure. A temporary or long-term account will need to be created, which the WSFC can facilitate.

At a minimum, the following data will be collected (see hardcopy in **Appendix B**):

- ✓ Agency name and Point of Contact information (name, telephone, email)
- ✓ Incident date and time
- ✓ How was the incident identified (IDS, audit log analysis, system administrator)
- ✓ Impact to agency
- ✓ What actions have already been taken
- ✓ Resources requested
- ✓ Resolution

In addition to the above information, the WSFC utilizes information found on the Network Incident Worksheet included in **Appendix C** – DOJ Cyber Task Force (CTF) Compromised Computer Network Incident Worksheet. All incident response teams will utilize this form when reporting incidents to the WSFC. Depending on the criticality it is not always feasible to gather all the information prior to reporting, but to continue to report information as it is collected.

4.0 SUBMISSION, ANALYSIS, AND DISSEMINATION

4.1 Analysis of Agency Incident/Event Data

Once information is received as discussed above it is analyzed in-house based on WSFC best practices, technical tools, defined processes and procedures, and considered for dissemination to the appropriate organizations or regulatory agencies. All reports of incidents and events received are triaged and reviewed upon receipt. Upon confirmation of incidents or events having a high severity rating, the WSFC will directly communicate to the reporting agency as well as all affected agencies to provide a status update and suggested mitigation or response activities.

Table 4-1 Essential Elements of Information

Vulnerability	Exploit	Emerging Threat
Is the vulnerability widely known?	Method & speed of propagation	Is the threat unique?
Is exploitation of the vulnerability being reported to incident response?	Protocol & ports	Does current anti-virus signatures detect the threat (are anti-virus vendors developing new signatures to protect against the threat?)
Is the Internet infrastructure at risk?	Payload; how destructive is it?	Is this repetitive of prior attacks?
What is the number of Internet systems at risk?	How many units are known to be affected?	Likely impact to a significant part of the Internet community
What is the impact on users of exploiting the vulnerability?	Relatively speaking, how important are the systems affected?	Visibility in the press
How easy is it to exploit the vulnerability?	How many unique sites or reporters have informed us of this activity?	See also the factors for Exploit.
What is the previous access required to exploit?	What is the localized impact of this activity during the incident?	
Visibility in the press	What is the residual impact of this activity after the incident?	
	How complicated is the attack method	
	Visibility in the press	

This assessment methodology is progressive. When relevant information is received concerning a unique security event or incident, its severity rating is assigned or reassessed with the receipt of updated or new information as the event progresses. The nature of the information and its severity rating dictates the actions taken by your organization and the dissemination and communications of the WSFC.

4.2 Severity Rating

It is important to use a standardized, repeatable and reliable method to assess the criticality or severity of a new or emerging cyber security event. The initial step after gathering information is to assess its "severity" using a scale from 1 to 5, with 1 being minimal and 5 being a crisis. Factors that are weighed in determining the 'severity' of a security event are based upon the following matrix:

Table 4-2 Severity Rating

Severity	Rating	Description
Minimal	1	Negligible impact on the organization.
Low	2	Very low impact on the organization. Unlikely to affect other organizations.
Medium	3	Poses a potential impact on the organization. Minimal possibility of impact to other organizations.
High	4	Has impacted the organization. Likely impact to other organizations.
Crisis	5	Has had a severe impact on the operational capacity of the organization. Known or expected impact to other organizations.

4.3 Cyber Insider Alert and Notification Publications

The United States Computer Emergency Readiness Team (US-CERT) releases technical alerts, analysis reports, bulletins outlining significant events and corresponding patches for vulnerabilities, current activity, and outreach tips to include information from the Multi-State Information Sharing & Analysis Center (MS-ISAC) and the National Cybersecurity and Communications Integration Center (NCCIC). Individuals can subscribe via email at https://www.us-cert.gov/

The Association of County and City Information Systems (ACCIS) is an organization composed of the Chief Information Systems Officers of Counties and Cities from within the State of Washington, who also welcome State Agencies, Districts, Commissions, and Ports as affiliate members. Their goals are to promote a communication link between the Information Systems functions of the member agencies; represent County and City Information Systems' interests to State officials, and to call attention to legislation affecting data processing operations and technology; and provide education for County and City officers on roles and responsibilities of Information Systems departments. ACCIS shares knowledge and expertise with other government IT professionals via Listserv and through semi-annual conferences. Visit https://www.accis-wa.org/ for further details and to apply for membership.

IT Security Daily Blasts are curated by Mike Hamilton, founder and CISO of CI Security, who has decades of experience in the Information Security industry. In that time, he has developed a keen eye for IT news that affects how security professionals approach their jobs and the news that will have meaningful impacts on daily life. Every weekday, Mike curates the top news stories in cybersecurity, including the latest breaches, security alerts, and industry developments. Sign up

for the *Daily Blast* and get it delivered early weekday mornings, at https://ci.security/news/daily-news

4.3.1 WSFC Products Related to Cyber Incident Response

At the heart of WSFC's mission is the need to share, on a real-time basis, relevant cyber security information with the organizations. Following this CONOPS the final state of the incident management process is dissemination of information.

Currently the WSFC utilizes the Northwest Warning Alert and Response Network (NWWARN) and Homeland Security Information Network (HSIN) to communicate with vetted critical infrastructure stakeholders from across the state. NWWARN was formed in partnership with the Pacific Northwest Economic Region as a way to connect public and private sector stakeholders from all critical infrastructure sectors. The fusion center currently vets new members of NWWARN and organizes stakeholders by sector. Vetted stakeholders can also send messages through the NWWARN system to share information. Currently there are over 3500 vetted stakeholders from all sectors across Washington and the surrounding region in the NWWARN database. The fusion center will utilize NWWARN as a primary way to communicate with specific sectors and jurisdictions regarding threats and warnings related to cyber incidents as well as HSIN for sensitive information sharing.

Monthly, the WSFC creates a report of the incidents that have been reported, their severity, time to resolve, and categories. This often includes a trend graph that will show incident trends over time based on category/severity.

4.4 Onsite Incident Response to Agencies

Request resources and specific cyber response assistance as needed based on the severity of the incident, assessment, and triage utilizing the agencies listed below.

Utilize agency-specific internal resolution and incident escalation processes first and foremost.

The National Guard's 10-person Cyber Civil Support Team can be activated via the request process through Pierce County Emergency Management's Duty Officer—which may or may not warrant a proclamation from the Pierce County Executive—which goes to the State Emergency Operations Center's (SEOC) Duty Officer, who then requests the Governor to activate the Team for additional support under United States Code, Title 32. The Governor can make an emergency declaration to access funding and can grant verbal approval to activate the National Guard. The team may also be activated under United States Code, Title 10. This type of assistance is comparatively high-priced and 'at-cost' to the requesting agency and should be considered in addition to the resources outlined in the below table.

Similarly, the Cyber Incident Response Coalition and Analysis Sharing (CIRCAS) group is a regional organization that is similar to the ISAC model (sector-specificity at the federal level). 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 Unified Coordination Group or support to ESF2 activities during State EOC activation. This is a private-sector equivalent of the mutual aid mechanism that is commonly exercised and utilized during emergency operations.

****Note**** Cyber is a unique arena where asset response can bypass the local and state processes and be requested directly to federal sources from local agencies. Notification to state and local emergency management is requested as a professional courtesy in the case federal assets are being deployed to Pierce County so appropriate accommodations can be made. The types of response outlined by PPD-41 consist of:

Threat Response – attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity to include conducting criminal investigations and other actions to counter the malicious cyber activity.

Asset Response – protecting assets and mitigating vulnerabilities in the face of malicious cyber activity to include reducing the impact to systems and or data; strengthening, recovering, and restoring services; identifying other entities at risk; and assessing potential risk to the broader community.

Table 4.4 – Reporting and Response Resources

Name	Phone	Email	Report	Threat Response	Asset Response
SSRIG	253-573-2434	PCINTEL@piercecountywa.gov	X		
WSFC	877-843-9522	intake@wsfc.wa.gov http://www.wsfc.wa.gov/Report	X	X	
MS-ISAC SOC 24/7	866-787-4722	soc@msisac.org	X		X
MS-ISAC = Multistate Information Sharing and Analysis Center *Report suspected or confirmed cyber incidents;* ***assistance to State, Local, Tribal, Territorial governments*** *in removal and restoring operations.* See **Appendix I** for further details.					
Ronald Watters Jr. **DHS IP Region X Cybersecurity Advisor**	206-348-4071	Ronald.watters@hq@dhs.gov		X	X
Pierce County Duty Officer 24/7	253-798-7470	PCEOC@piercecountywa.gov ***(PENDING)*			X**
State Duty Officer 24/7 and Natl' Guard	800-258-5990	Dutyofficer@mil.wa.gov ****(proclamation required)**			X**
NCCIC	888-282-0870	WatchandWarning@hq.dhs.gov			X
NCCIC = National Cybersecurity and Communications Integration Center *Report suspected or confirmed cyber incidents;* ***government assistance*** *in removal and restoring operations.*					
US Secret Service Seattle Field Office	206-553-1922	Seattle.fbi@ic.fbi.gov		X	
Theft of payment card or other ***financial information.***					

4.5 Incident Escalation

Escalation criteria are based on actual operational incident reports received and analysis performed by the WSFC. These criteria will best indicate an incident which has operational significance throughout the local cyber community. WSFC has responsibility for maintaining and updating the list below and for publishing updates to reporting agencies as necessary. Factors are weighed and verified in determining the severity of an incident based upon the following criteria:

Table 4-5 Escalation Criteria

Escalation Criteria
Any intrusion into a classified network.
Any unauthorized privileged user, administrator, or root level access of a system which crosses organization or agency boundaries.
Any incident involving a second level domain name server.
Any incident which impacts an organization's operations.
Any incident from a country against which the US is currently conducting operations or will imminently conduct operations.
Any targeted intrusion of the critical infrastructure or government networks.
Any incident involving a second level domain web server
Any new virus/worm for which no published countermeasure exists, any new virus/worm whose propagation could likely circumvent organization's containment capabilities, or any new virus/worm which affects vital network services (e.g., e-mail and DNS services).
Any root level access on a system using new methods, which exploit significant vulnerabilities shared across organization or third-party systems.

4.6 Notification of Other Related Organizations, Emergency Management, and Law Enforcement

WSFC will continue to work directly with the organizational and community incident response teams that includes CIRCAS, law enforcement, intelligence community, and other related public and private sector organizations to assess the situation and continually update all parties as appropriate.

Some of these organizations will need to know an incident occurred and what its potential operational impact is at the local, state, or national level, if any. Other organizations will require more technical detail to help them better protect their information assets for which they are responsible.

4.7 Communications

During a cybersecurity incident, consider all regulatory requirements for reporting in addition to implementing your agency's Continuity of Operations Plan (COOP) outlining phone trees of internal and external communication and notification. Consider verifying traffic or alert and notification with vendors, contractors, consultants, and internal staff and leadership. Your agency insurance company may have response assets available for the recovery process.

4.7.1 Communication Guidelines

The matrix below provides general guidance but at the discretion of the WSFC analyst it should be considered flexible and dynamically adjustable as appropriate to the specific incident.

Table 4-7 Communication Guidance

Severity Rating	Notifications To
Minimal (1)	Internal to organization, SSRIG, and WSFC or other analyst personnel
Low (2)	All the above and outside analysts, Local and State agencies (WA EMD, CISO, Attorney General)
Medium (3)	All the above and Regulatory (NERC/FERC, USCG, SEC) and Federal Agencies (DHS NCIC, FBI, USSS, ATF, US Attorney) **If an organization is regulated, they must directly notify the regulatory body**
High (4)	All the above and other similar organizations
Crisis (5)	All the above and CIRCAS, ISACs, ISAOs, other information sharing organizations.

4.8 Regulatory Requirements

Organizations may have specific regulatory reporting requirements. It is outside the scope of this CONOPS to detail all of those, however each organization must be cognizant and compliant with any required regulatory notice protocols. Many of these are referenced in **Appendix A**.

5.0 SECURING AND SAFEGUARDING INFORMATION

Participating organizations may expect or require that their identifying information and any specific intellectual property or other sensitive security information be protected as part of this process.

5.1 Confidentiality

Systems of collection and retention of cyber incident information will be designed to ensure confidentiality of attribution and will have mechanisms with which participating organizations can select which data is shared and with whom. Stakeholders are encouraged to use the Traffic Light Protocol as defined by US CERT. https://www.us-cert.gov/tlp The Traffic Light Protocol (TLP) was created to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). See **Appendix D**.

5.2 Outreach and education

PCEM will partner with the WSFC, Washington State EMD, city emergency management, IT, law enforcement, public and private sector, academia, healthcare, and critical infrastructure partners from across the region to provide update on training opportunities and to promote the CONOPS.

APPENDIX A REGULATORY REQUIREMENTS

Types	Industry Groups
1. Security	▪ PCI, FINRA
2. Privacy	Federal Laws & Regulations
3. Unauthorized Access	▪ HIPAA, GLBA, FERPA
International Laws	▪ FTC, SEC, FCC, HHS
▪ Privacy Shield	
▪ GDPR	

1. North American Electric Reliability Corporation (NERC)/Federal Energy Regulatory Commission (FERC). There are 14 mandatory NERC standards.
   https://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States
   Critical Infrastructure Protection (CIP) establishes requirements for securing the bulk power system with 11 reliability standards subject to enforcement. NERC CIP Standards 002–009 – NERC for entities responsible for the availability and reliability of the bulk electric system.

2. United State Coast Guard (USCG) Navigation and Vessel Inspection Circular (NVIC) 05-17; Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities https://www.regulations.gov/document?D=USCG-2016-1084-0002
   Entities that are regulated under the Maritime Transportation Security Act (MTSA) are also subject to the NVIC. Entities must be able to demonstrate how they are addressing cyber security risks. The NVIC also establishes best practices and expectations.

3. Securities and Exchange Commission (SEC) https://www.sec.gov/spotlight/cybersecurity
   Commission Statement and Guidance on Public Company Cybersecurity Disclosures

4. Health Insurance Portability and Accountability Act (HIPAA)/ Health Information Technology for Economic and Clinical Health Act (HITECH)
   https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

5. Privacy Technical Assistance Center (PTAC)—created by the US Department of Education—is a resource for cyber security issues in education. PTAC's Data Breach Response Checklist:
   https://studentprivacy.ed.gov/sites/default/files/resource_document/file/checklist_data_breach_response_092012_0.pdf

6. Criminal Justice Information Services (CJIS/FBI) Security Policy
   The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, storage, and destruction of CJI. This policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.
   https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

7. General Data Protection Regulation (GDPR)
   Applies to companies that store or process the personal information of EU citizens in EU states. The regulation is consistent across all 28 EU states. Per Article 33 of the GDPR, organizations have 72 hours after learning of a data breach to report it.
   https://www.eugdpr.org/
   https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

8. PCI Data Security Standards (PCI DSS)—security of cardholder data
   Helps protect the safety of cardholder data that is stored, processed or transmitted. They set the operational and technical requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions.
   https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

9. 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.

10. Revised Code of Washington, Chapter 42.56: Public Records Act
    http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56
    RCW 42.56.590 - Personal information—Notice of security breaches.
    RCW 43.43.856 - Divulging investigative information prohibited—Confidentiality—Security of records and files

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

12. 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. http://csrc.nist.gov/publications/PubsSPs.html

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

14. AMI System Security Requirements: Security requirements for advanced metering infrastructure.
    http://energy.gov/oe/downloads/ami-system-security-requirements-v101-1

15. IEEE (Institute of Electrical and Electronics Engineers) 1686-2007, Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
    http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4453853&queryText%3DStandard+for+Substation+Intelligent+Electronic+Devices)

APPENDIX B

WASHINGTON STATE FUSION CENTER SUSPICIOUS ACTIVITY REPORT

REPORT SUSPICIOUS ACTIVITY

Important: If this is an emergency, call 911

Your Contact Information (Optional)

I am a:

- ☐ Private Citizen
- ☐ Law Enforcement Officer
- ☐ Private Security
- ☐ Critical Infrastructure
- ☐ First Responder
- ☐ Other

First Name: _____

Last Name: _____

Email Address: _____

Agency/Org: _____

Phone: _____

Type of Information

Type of Information:

- ☐ Suspicious Person
- ☐ Possible Crime
- ☐ Event
- ☐ Suspicious Activity
- ☐ General Information
- ☐ Other

How did you obtain this information? (for example, direct observation, from a third party, etc.)

_____

_____

REPORT SUSPICIOUS ACTIVITY

Important: If this is an emergency, call 911

Incident or Event Details

Incident/Event Type (see type descriptions on final page)**:**

These activities are generally first amendment-protected activities. All reported activity will be reviewed to ensure that civil rights and liberties are protected and the information meets the WSFC privacy policy.

Defined Criminal Activity and Potential Terrorism Nexus Activity

Potential Criminal or Non-Criminal Activity Requiring Additional Fact Information During Investigation

- ☐ **Breach/Attempted Intrusion**
- ☐ **Misrepresentation**
- ☐ **Theft/Loss Diversion**
- ☐ **Eliciting Information**
- ☐ **Sabotage/Tampering/Vandalism**
- ☐ **Testing or Probing of Security**
- ☐ **Cyber Attack**
- ☐ **Photography**
- ☐ **Aviation Activity**
- ☐ **Operation/Surveillance**
- ☐ **Expressed or Implied Threat**
- ☐ **Recruiting**
- ☐ **Materials Acquisition/Storage**
- ☐ **Acquisition of Expertise**
- ☐ **Weapons Discovery**

Approximate Date: _____

Approximate Time: _____:_____ AM / PM

REPORT SUSPICIOUS ACTIVITY

Important: If this is an emergency, call 911

Description of incident or event (what did you see, hear, or learn about?):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Location/Area affected (please include as much detail as possible: street, city, state, zip or a description of the location where the incident occurred):

_____
_____
_____
_____
_____
_____

Why do you believe this is unusual or suspicious?

_____
_____
_____
_____
_____
_____
_____

REPORT SUSPICIOUS ACTIVITY

Important: If this is an emergency, call 911

Information About Involved Persons

Name, Height, Distinguishing Scars, Marks, Tattoos, Accents, Gait, or Mannerisms:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Information About Involved Vehicle/Vessel/Aircraft

Vehicle Color, Make, Model, License, Tail Number, Condition (new, old, dirty, broken window, etc.) or anything else that describes the vehicle:

_____
_____
_____
_____
_____
_____
_____

SUBMIT TO:

South Sound Regional Intelligence Group (SSRIG)
253-573-2434 | PCINTEL@piercecountywa.gov

Washington State Fusion Center (WSFC)
877-843-9522 | intake@wsfc.wa.gov

Direct online reporting: http://www.wsfc.wa.gov/Report

REPORT SUSPICIOUS ACTIVITY

Important: If this is an emergency, call 911

Reporting Information & Guidelines

"We're all safer when local law enforcement works together with the communities and citizens they serve, and their partners in the Federal government. It's a simple but powerful, idea - that homeland security begins with hometown security. And there's a role for all of us." Secretary Janet Napolitano, Department of Homeland Security

In July 2010, the Department of Homeland Security (DHS), at Secretary Janet Napolitano's direction, launched a national "If You See Something, Say Something™" public awareness campaign –a simple and effective program to raise public awareness of indicators of terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper state and local law enforcement authorities.

Factors such as race, ethnicity, national origin, or religious affiliation alone are not suspicious. For that reason, the public should report only suspicious behavior and situations (e.g., an unattended backpack in a public place or someone trying to break into a restricted area) rather than beliefs, thoughts, ideas, expressions, associations, or speech unrelated to terrorism or other criminal activity. Only reports that document **behavior reasonably indicative of criminal activity related to terrorism** will be shared with federal, state, local and tribal partners.

Copyright ©2018 Washington State Fusion Center - All Rights Reserved

South Sound Regional Intelligence Group (SSRIG)
253-573-2434 | PCINTEL@piercecountywa.gov

Washington State Fusion Center (WSFC)
877-843-9522 | intake@wsfc.wa.gov

Protect your every day.

RECOGNIZE THE SIGNS

OF TERRORISM-RELATED SUSPICIOUS ACTIVITY

EXPRESSED OR IMPLIED THREAT
Threatening to commit a crime that could harm or kill people or damage a facility, infrastructure, or secured site

PHOTOGRAPHY/ SURVEILLANCE
Taking pictures or videos, or a prolonged interest in personnel, facilities, security features, or infrastructure in an unusual or covert manner

THEFT/LOSS/ DIVERSION
Stealing or diverting items—such as equipment, uniforms, or badges—that belong to a facility or secured site

TESTING OR PROBING OF SECURITY
Investigating or testing a facility's security or IT systems to assess the strength or weakness of the target

AVIATION ACTIVITY
Operating or interfering with the operation of an aircraft that poses a threat of harm to people and property

BREACH/ ATTEMPTED INTRUSION
Unauthorized people trying to enter a restricted area or impersonating authorized personnel

ACQUISITION OF EXPERTISE
Gaining skills or knowledge on a specific topic, such as facility security, military tactics, or flying an aircraft

ELICITING INFORMATION
Questioning personnel beyond mere curiosity about an event, facility, or operations

MISREPRESENTATION
Presenting false information or misusing documents to conceal possible illegal activity

CYBERATTACK
Disrupting or compromising an organization's information technology systems

RECRUITING/ FINANCING
Funding suspicious or criminal activity or recruiting people to participate in criminal or terrorist activity

SABOTAGE/ TAMPERING/ VANDALISM
Damaging or destroying part of a facility, infrastructure, or secured site

MATERIALS ACQUISITION/ STORAGE
Acquisition and/or storage of unusual materials such as cell phones, radio controllers, or toxic materials

WEAPONS COLLECTION/ STORAGE
Collection or discovery of unusual amounts of weapons including explosives, chemicals, or other destructive materials

SECTOR-SPECIFIC INCIDENT
Actions which raise concern to specific sectors, (e.g., power plant) with regard to their personnel, facilities, systems, or functions

If you **see** something, **say** something®

REPORT SUSPICIOUS ACTIVITY TO LOCAL AUTHORITIES OR CALL 9-1-1 IN CASE OF EMERGENCY

dhs.gov/see-something-say-something

APPENDIX C

DOJ CTF COMPROMISED COMPUTER NETWORK INCIDENT WORKSHEET

1. Organization Information	
Organization Name:	
Organization Address:	
Name of Person Reporting:	
Name of Network Administrator:	
Name of CISO:	
Name of CIO/Executive Level Decision Maker:	
Date of Report:	

2. What type of network compromise occurred? (please select all that apply)			
☐ Reconnaissance	☐ Malware	☐ Data Exfiltration	☐ Other (please describe)

3. What equipment has been impacted?	
Type:	
Manufacturer:	
Model Number:	
Serial Number:	

4. What operating system(s) was (were) installed on the equipment at the time of the intrusion?					
OS:		OS:		OS:	
Version:		Version:		Version:	
Time Zone:		Time Zone:		Time Zone:	

5. Are/Were software patches regularly installed?		
☐ Yes	☐ No	☐ Unknown

6. Does your network utilize any virtual machines or cloud services?		
☐ Yes – If so, which ones?	☐ No	☐ Unknown

7. Is remote connectivity enabled on your network?		
☐ Yes – Please select all that apply	☐ No	☐ Unknown
☐ SSH – Please provide which version:		
☐ Telnet – Please provide which version:		
☐ RDP – Please provide which version:		
☐ VPN – Please provide which version:		
☐ Other – Please provide type and version:		
8. Does your organization use any web services?		
☐ Yes – Please list all services in use	☐ No	
9. Please list all domain names associated with your network.		
10. Please provide your server's DHCP address.		
11. Does your organization maintain DCHP logs?		
☐ Yes – If so, where?	☐ No	☐ Unknown
12. Does your organization maintain web server logs?		
☐ Yes – If so, where?	☐ No	☐ Unknown
13. Please provide your organization's network DNS address.		
Is it internal or external to your organization?		
☐ Internal	☐ External	☐ Unknown
14. Please list the range of your organization's IP addresses.		
Of these, how many does your organization own and/or use?		
15. Does your organization maintain any data backups?		
☐ Yes – If so, where?	☐ No	☐ Unknown

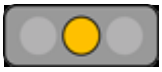
16. What terminal services are/were running on the impacted equipment?		
17. What ports are/were enabled on the impacted equipment?		
18. Does your organization own or operate any Wi-Fi access points?		
☐ Yes	☐ No	☐ Unknown
If so, are they active or passive?		
☐ Active	☐ Passive	
19. Do you suspect the unauthorized intrusion on your network to be the result of a current or former employee?		
☐ Yes	☐ No	
20. Are your employees informed of the limits of their acceptable use and privileges on your network?		
☐ Yes	☐ No	☐ Unknown
21. Are employees given any instructions related to the cessation of their network use and privileges when they leave employment or are terminated?		
☐ Yes	☐ No	☐ Unknown
22. Has your organization taken any steps to mitigate the impact of the intrusion?		
☐ Yes – if so, please describe	☐ No	☐ Unknown

23. To the best of your ability, please quantify your estimated financial loss as a result of this incident.*	
Equipment Loss:	
Equipment Repairs:	
New Equipment:	
New Software:	
Employee Overtime:	
Consulting Costs:	
Reputation Degradation:	
Customer/Business Loss:	

**** We understand that an intrusion event can, regrettably, result in an array of costs and financial losses to your company. We also understand that it can sometimes take weeks or months to determine the full scope of those costs/losses. We seek***

that information, as you are able to provide it, because it is relevant to a criminal investigation. It is particularly important in determining the sentence that we will seek, assuming a successful prosecution and conviction.
24. Please provide a diagram and narrative description of your network architecture and configurations that lists the location (city/state/country) of all servers and users on the network (see example).
25. Please provide the relevant usernames and passwords for all equipment impacted by the intrusion.

APPENDIX D TRAFFIC LIGHT PROTOCOL (TLP)

Color	When should it be used?	How may it be shared?
TLP:RED Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

APPENDIX E FEDERAL POINTS OF CONTACT

Cyber Incident Reporting

A Unified Message for Reporting to the Federal Government

Cyber incidents can have serious consequences. The theft of private, financial, or other sensitive data and cyber attacks that damage computer systems are capable of causing lasting harm to anyone engaged in personal or commercial online transactions. Such risks are increasingly faced by businesses, consumers, and all other users of the Internet.

A private sector entity that is a victim of a cyber incident can receive assistance from government agencies, which are prepared to investigate the incident, mitigate its consequences, and help prevent future incidents. For example, federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery. When supporting affected entities, the various agencies of the Federal Government work in tandem to leverage their collective response expertise, apply their knowledge of cyber threats, preserve key evidence, and use their combined authorities and capabilities both to minimize asset vulnerability and bring malicious actors to justice. This fact sheet explains when, what, and how to report to the Federal Government in the event of a cyber incident.

When to Report to the Federal Government

A cyber incident is an event that could jeopardize the confidentiality, integrity, or availability of digital information or information systems. Cyber incidents resulting in significant damage are of particular concern to the Federal Government. Accordingly, victims are encouraged to report all cyber incidents that may:

- result in a significant loss of data, system availability, or control of systems;
- impact a large number of victims;
- indicate unauthorized access to, or malicious software present on, critical information technology systems;
- affect critical infrastructure or core government functions; or
- impact national security, economic security, or public health and safety.

What to Report

A cyber incident may be reported at various stages, even when complete information may not be available. Helpful information could include who you are, who experienced the incident, what sort of incident occurred, how and when the incident was initially detected, what response actions have already been taken, and who has been notified.

How to Report Cyber Incidents to the Federal Government

Private sector entities experiencing cyber incidents are encouraged to report a cyber incident to the local field offices of federal law enforcement agencies, their sector specific agency, and any of the federal agencies listed in the table on page two. The federal agency receiving the initial report will coordinate with other relevant federal stakeholders in responding to the incident. If the affected entity is obligated by law or contract to report a cyber incident, the entity should comply with that obligation in addition to voluntarily reporting the incident to an appropriate federal point of contact.

Types of Federal Incident Response

Upon receiving a report of a cyber incident, the Federal Government will promptly focus its efforts on two activities: Threat Response and Asset Response. Threat response includes attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. It includes conducting criminal investigations and other actions to counter the malicious cyber activity. Asset response includes protecting assets and mitigating vulnerabilities in the face of malicious cyber activity. It includes reducing the impact to

systems and/or data; strengthening, recovering and restoring services; identifying other entities at risk; and assessing potential risk to the broader community.

Irrespective of the type of incident or its corresponding response, Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

Key Federal Points of Contact	
Threat Response	***Asset Response***
Federal Bureau of Investigation (FBI) **FBI Field Office Cyber Task Forces:** http://www.fbi.gov/contact-us/field **Internet Crime Complaint Center (IC3):** http://www.ic3.gov *Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.* *Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.*	National Cybersecurity and Communications Integration Center (NCCIC) **NCCIC:** (888) 282-0870 or NCCIC@hq.dhs.gov **United States Computer Emergency Readiness Team:** http://www.us-cert.gov *Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.*
National Cyber Investigative Joint Task Force **NCIJTF CyWatch 24/7 Command Center:** (855) 292-3937 or cywatch@ic.fbi.gov *Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of federal law enforcement agencies or the Federal Government.*	
United States Secret Service **Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs):** http://www.secretservice.gov/contact/field-offices *Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information*	
United States Immigration and Customs Enforcement / Homeland Security Investigations (ICE/HSI) **HSI Tip Line:** 866-DHS-2-ICE (866-347-2423) or https://www.ice.gov/webform/hsi-tip-form **HSI Field Offices:** https://www.ice.gov/contact/hsi **HSI Cyber Crimes Center:** https://www.ice.gov/cyber-crimes *Report cyber-enabled crime, including: digital theft of intellectual property; illicit e-commerce (including hidden marketplaces); Internet-facilitated proliferation of arms and strategic technology; child pornography; and cyber-enabled smuggling and money laundering.*	
If there is an immediate threat to public health or safety, the public should always call 911.	

APPENDIX F LIST OF ACRONYMS

ACCIS	Association of County and City Information Systems
CEMP	Comprehensive Emergency Management Plan
CERT	Computer Emergency Response Teams
CHRI	Criminal History Record Information
CIKR	Critical Infrastructure and Key Resources
CIP	Critical Infrastructure Protection
CIRCAS	Cyber Incident Response Coalition and Analysis Sharing
CISO	Chief Information Security Officer
CJI	Criminal Justice Information
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
CSA	Cyber Security Advisor
CTF	Cyber Task Forces
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DHS IP	Department of Homeland Security Office of Infrastructure Protection
DOJ	Department of Justice
DoS	Denial of Service
E911	Enhanced 9-1-1
FBI	Federal Bureau of Investigation
HSA	Homeland Security Advisor
HSIN	Homeland Security Information Network
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IoT	Internet of Things
IP	Internet Protocol
IRP	Incident Response Plan
IT	Information Technology
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCCIC	National Cybersecurity and Communications Integration Center
NGO	Nongovernmental Organizations
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NOC	National Operations Center
NRF	National Response Framework
NWWARN	Northwest Warning Alert and Response Network
PCEM	Pierce County Emergency Management
PCI	Payment Card Industry
PII	Personally Identifiable Information

PPD	Presidential Policy Directive
PSAP	Public Safety Answering Points
SCADA	Supervisory Control and Data Acquisition
SEOC	State Emergency Operations Center
SOC	Security Operations Center
SSRIG	South Sound Regional Intelligence Group
TLP	Traffic Light Protocol
US-CERT	United States Computer Emergency Readiness Team
WSFC	Washington State Fusion Center

APPENDIX G CYBER SECURITY GLOSSARY

A

antivirus

Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

APT (Advanced Persistent Threat)

A set of stealthy and continuous computer backing processes, often orchestrated by human(s) targeting a specific entity. APT usually targets nations or organizations for business or political motives.

attacker

Malicious actor who seeks to exploit computer systems with the intent to change, destroy, steal or disable their information, and then exploit the outcome.

B

Bitcoin

Digital currency that can be transferred instantly and securely anywhere in the world. Bitcoin is used for paying ransom because its quick, easy, and can be difficult to trace the hackers.

botnets (robot-networks)

A network of devices infected with Trojan horse viruses, connected to the Internet, used to commit coordinated cyber-attacks without their owner's knowledge and controlled remotely by a hacker. Risks include: DoS attacks, malware distribution, and or intelligence gathering.

blended attack

An attack that contains both a cyber-based attack as well as a physical attack.

breach

An incident in which data, computer systems or networks are accessed or affected in a non-authorized way.

browser

A software application which presents information and services from the web.

brute force attack

Using a computational power to automatically enter a huge number of combination of values, one-by-one, usually in order to discover passwords and gain access.

Bring Your Own Device (BYOD)

An organization’s strategy or policy that allows employees to use their own personal devices for work purposes.

C

certificate

A form of digital identity for a computer, user or organization to allow the authentication and secure exchange of information.

cloud

Where shared compute and storage resources are accessed as a service (usually online), instead of hosted locally on physical services. Resources can include infrastructure, platform or software services.

credentials

A user's authentication information used to verify identity - typically one, or more, of password, token, certificate.

cyber attack

Malicious attempts to damage, disrupt or gain unauthorized access to computer systems, networks or devices, via cyber means.

cyber incident

An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive [PPD-41], a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. **Significant cyber incident.** A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

cyber preparedness

The process of ensuring that an agency, organization, or jurisdiction has developed, tested, and validated its capability to protect against, prevent, mitigate, respond to, and recover from a significant cyber incident.

cyber security

The activity or process of defending information and communications systems and the information contained within them from damage, unauthorized use or modification, or exploitation.

D

data breach

An event in which an individual’s name plus a medical record and or a financial record or debit/credit card is potentially put at risk—either in electronic or paper format.

dictionary attack

A type of *brute force attack* in which the attacker uses known dictionary words, phrases or common passwords as their guesses.

digital footprint

A 'footprint' of digital information that a user's online activity leaves behind.

Denial of Service (DoS)

When legitimate users are denied access to computer services (or resources), or the delaying of time-critical operations usually by overloading the service with requests.

Distributed Denial of Service (DDos)

A denial of service technique that uses numerous hosts to perform the attack.

download attack

The unintentional installation of malicious software or virus onto a device without the users knowledge or consent. May also be known as a drive-by download.

E

encryption

A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

End User Device (EUD)

Collective term to describe modern smartphones, laptops and tablets that connect to an organization's network.

exploit

May refer to software or data that takes advantage of a vulnerability in a system to cause unintended consequences.

F

firewall

Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorized access to or from a network.

H

hacker

In mainstream use as being someone with some computer skills who uses them to break into computers, systems and networks.

Hacktivists: Common term for hackers with a political agenda.

honeypot (honeynet)

Decoy system or network to attract potential attackers that helps limit access to actual systems by detecting and deflecting or learning from an attack. Multiple honeypots form a honeynet.

I

incident

A breach of the security rules for a system or service, such as:

- attempts to gain unauthorized access to a system and/or data
- unauthorized use of systems for the processing or storing of data
- changes to a systems firmware, software or hardware without the system owners consent
- malicious disruption and/or denial of service

Industrial Control System

An information system used to control industrial processes such as manufacturing, product handling, production, and distribution tor to control infrastructure assets.

insider risks

The potential for damage to be done maliciously or inadvertently by a legitimate user with privileged access to systems, networks or data.

Internet of Things (IoT)

Refers to the ability of everyday objects (rather than computers and devices) to connect to the Internet. Examples include kettles, fridges and televisions.

Internet Protocol (IP)

The method or protocol by which data is sent from one computer to another on the Internet.

M

macro

A small program that can automate tasks in applications (such as Microsoft Office) which attackers can use to gain access to (or harm) a system.

major cyber incident (as defined by the US Federal Cybersecurity Centers)

Any incident that is **likely to result in demonstratable impact** to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people (Level 3 – Orange, or higher)

- Severe, Level 4 incident (red): is "**likely to result in a significant impact** to public health or safety, national security, economic security, foreign relations, or civil liberties."
- Emergency, Level 5 incident (black): "**poses an imminent threat** to the provision of wide-scale critical infrastructure services, national government stability, or the lives of US persons."

malvertising

Using online advertising as a delivery method for malware.

malware

Malicious software - a term that includes viruses, trojans, worms or any code or content that could have an adverse impact on organizations or individuals.

mitigation

Steps that organizations and individuals can take to minimize and address risks.

N

network

Two or more computers linked in order to share resources.

P

patching

Applying updates to firmware or software to improve security and/or enhance functionality.

pen test

Short for *pene*tration *test*. An authorized test of a computer network or system designed to look for security weaknesses so that they can be fixed.

pharming

An attack on network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct address.

phishing

Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

platform

The basic hardware (device) and software (operating system) on which applications can be run.

R

ransomware

Malicious software that makes data or systems unusable until the victim makes a payment.

router

A network device which sends data packets from one network to another based on the destination address. May also be called a gateway.

S

SCADA (Supervisory Control and Data Acquisition)

A catchall term used in the United States to describe those IT systems that are used to govern infrastructure elements (most often public utilities).

software as a service (SaaS)

Describes a business model where consumers access centrally-hosted software applications over the Internet.

sanitization

Using electronic or physical destruction methods to securely erase or remove data from memory.

smishing

Phishing via SMS: mass text messages sent to users asking for sensitive information (e.g. bank details) or encouraging them to visit a fake website.

social engineering

Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

spear-phishing

A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

spoof/spoofing/spoofed

Term meaning “falsified” or “obscured.” Often used in conjunction with terms describing specific forms or techniques of communication (e.g., “IP spoofing,” “spoofed email addresses,” “spoofed” telephone number”).

T

trojan

A type of malware or virus disguised as legitimate software, that is used to hack into the victim's computer.

Traffic Light Protocol (TPL)

A set of designations employing four colors—RED, AMBER, GREEN, and WHITE) used to ensure that sensitive information is shared with the correct audience.

two-factor authentication (2FA)

The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

V

virus

Programs which can self-replicate and are designed to infect legitimate software programs or systems by infecting host computers through downloads, email attachments, or removable media such as CDs, DVDs, or USB drives. A form of malware.

vishing

A social engineering attack in which the victim is convinced to give up information over a telephone (often involving Voice Over IP (VoIP) technology).

VoIP (Voice over IP)

A set of technologies that utilize Internet Protocol (IP) to facilitate telephone communications, as opposed to legacy telecommunications equipment.

Virtual Private Network (VPN)

An encrypted network often created to allow secure connections for remote users, for example in an organization with offices in multiple locations.

vulnerability

A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorized access to a system.

W

water-holing (watering hole attack)

Setting up a fake website (or compromising a real one) in order to exploit visiting users.

war driving

The act of using a portable computer device to locate wireless networks when in a moving vehicle.

web-based attacks

Techniques that redirect the browser to malicious sites taking advantage of known vulnerabilities in programming code and scripting or poorly secure web forms like a comment field on a blog.

whaling

Highly targeted phishing attacks (masquerading as a legitimate emails) that are aimed at senior executives.

whitelisting

Authorizing approved applications for use within organizations in order to protect systems from potentially harmful applications.

worm

A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

Z

zero-day attack

A cyber-attack which exploits undisclosed or unpatched computer application vulnerabilities. Zero-day attacks can be considered extremely dangerous because they take advantage of computer security holes for which no solution is currently available.

zero-day exploit

An exploit that takes advantage of a security risk on the same day that this risk becomes public.

zombie

An infected computer that is remotely controlled by a hacker and is part of a large group of compromised computers called a botnet. Zombies are commonly used to send spam, launch denial-of-service attacks, and infect other systems.

APPENDIX H CYBERSECURITY DOCTRINE AND RESOURCES

Principal Doctrine

- Comprehensive National Cybersecurity Initiative (CNCI) http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative
- Cybersecurity: Authoritative Reports and Resources (Congressional Research Service) http://www.fas.org/sgp/crs/misc/R42507.pdf
- Cyberspace Policy Review http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
- National Cyber Incident Response Plan (NCIRP) (2016) https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf
- Executive Order: Improving Critical Infrastructure Cybersecurity (2013) http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
- Framework for Improving Critical Infrastructure Cybersecurity (2014) http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
- Homeland Security Presidential Directive (HSPD 7) https://www.dhs.gov/homeland-security-presidential-directive-7
- National Institute of Standards and Technology Computer Security Incident Handling Guide http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf
- National Strategy for Trusted Identities in Cyberspace (2011) http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
- National Strategy to Secure Cyberspace (2003) https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2013) http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- Presidential Policy Directive 41: United States Cyber Incident Coordination (2016) https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

Department of Homeland Security

Cyber Capabilities/Entities

- National Cybersecurity and Communications Integration Center (NCCIC) (contact: NCCIC@hq.dhs.gov)
  - Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (contact: ics-cert@hq.dhs.gov; 877-776-7585)
  - National Coordinating Center for Communications (NCC) (contact: NCC@hq.dhs.gov; 703-235-5080)
  - United States Computer Emergency Readiness Team (US-CERT) (contact: info@us-cert.gov; 888-282-0870)
- National Infrastructure Coordinating Center (contact: NICC@hq.dhs.gov)

Resources/Documents

- Understanding Federal Cybersecurity
  https://www.belfercenter.org/sites/default/files/files/publication/Understanding%20Federal%20Cybersecurity%2004-2018_0.pdf
- Cyber Storm III Final Report
  http://www.dhs.gov/sites/default/files/publications/nppd/CyberStorm%20III%20FINAL%20Report.pdf
- DHS Blueprint for a Secure Cyber Future
  http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf
- DHS Memorandum of Agreement with Department of Defense
  http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf
- DHS Quadrennial Homeland Security Review
  http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf
- DHS Strategic Plan Fiscal Years 2012-2016
  https://www.dhs.gov/sites/default/files/publications/DHS%20Strategic%20Plan.pdf
- Enabling Distributed Security in Cyberspace
  http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf
- ICS-CERT Incident Response Summary Report 2009-2011
  http://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT%20Incident%20Response%20Summary%20Report%20%282009-2011%29.pdf
- National Infrastructure Protection Plan (NIPP) 2013
  http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience
- National Response Framework (NRF)
  http://www.fema.gov/national-response-framework
- NCCIC, US-CERT, ICS-CERT Fact Sheets
  ICS-CERT: http://ics-cert.us-cert.gov/sites/default/files/DHS_CyberSecurity_ICSCERT-FactSheet-v8.pdf
- Protected Critical Infrastructure Information (PCII) Program Fact Sheet
  http://www.dhs.gov/xlibrary/assets/pcii/dhs-ip-pcii-fact-sheet.pdf
- Testimony of NCCIC Director Seán P. McGurk, National Protection and Programs Directorate, before the U.S. House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, "*The DHS Cybersecurity Mission: Promoting Innovation and Securing Critical Infrastructure*."
  http://www.dhs.gov/ynews/testimony/testimony_1302814781943.shtm
- Written testimony of Department of Homeland Security Secretary Janet Napolitano for a Senate Committee on the Judiciary hearing titled, "*The Oversight of the Department of Homeland Security*."
  http://www.dhs.gov/ynews/testimony/20120425-s1-dhs-oversight-sjc.shtm

Washington State & Pierce County Government

Cyber Capabilities/Entities

- Association of County and City Information Systems https://www.accis-wa.org/
- Washington State | Office of the Chief Information Officer https://ocio.wa.gov/
- Washington Technology Solutions (WaTech) https://watech.wa.gov/
- Washington State Emergency Management Division, Cybersecurity Program https://www.mil.wa.gov/emergency-management-division/cyber-security-program
- MS-ISAC (contact: info@msisac.org; 518-266-3460)

Resources/Documents

- Washington State Hazard Profile, Cyber Threat (Oct 2015) https://mil.wa.gov/uploads/pdf/hazplancyber.pdf
- Cybersecurity Governance in the State of Washington: A Case Study (Dec 2017)
- https://www.us-cert.gov/sites/default/files/c3vp/sltt/Washington_Cyber_Governance_Case_Study_508.pdf
- Resources for State, Local, Tribal, and Territorial (SLTT) Governments https://www.us-cert.gov/ccubedvp/sltt
- The Significant Cyber Incident Annex to the Washington State Comprehensive Emergency Management Plan—Annex D https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf
- Cyber Incident Annex to the Pierce County Comprehensive Emergency Management Plan – Incident Annex 3 https://www.co.pierce.wa.us/DocumentCenter/View/35761/IA3-2014-Final?bidId=
- Call to Action: Cybersecurity and the States (National Association of State Chief Information Officers [NASCIO]) http://www.nascio.org/advocacy/current/NASCIO_Cybersecurity_Call_to_Action_Final.pdf
- MS-ISAC Charter https://msisac.cisecurity.org/about/charter/documents/MS-ISACCharter2013-03.pdf
- MS-ISAC Cyber Incident Response Guide: A Non-Technical Guide http://msisac.cisecurity.org/members/local-government/documents/FINALIncidentResponseGuide.pdf

Private Sector/Business

Cyber Capabilities/Entities

- Business Executives for National Security http://www.bens.org/
- Electronic Privacy Information Center http://epic.org/
- Internet Security Alliance http://www.isalliance.org/
- National Council of ISACs http://www.isaccouncil.org/
- Partnership for Critical Infrastructure Security http://insidecybersecurity.com/iwpfile.html?file=pdf13/cs09102013_PCIS_Proposal_Effective_Public_Private_Partnership.pdf

Resources/Documents

- Resources for Small and Midsize Businesses (SMB), US-CERT https://www.us-cert.gov/ccubedvp/smb
- Resources for Business (US-CERT) https://www.us-cert.gov/ccubedvp/business
- Commonsense Guide to Cyber Security for Small Businesses (U.S. Chamber of Commerce) http://www.ready.gov/sites/default/files/documents/files/security_for_small_business%5B1%5D.pdf
- The Financial Management of Cyber Risk (ANSI and Internet Security Alliance) http://publicaa.ansi.org/sites/apdl/khdoc/Financial+Management+of+Cyber+Risk.pdf
- The Role of ISACs in Private/Public Critical Infrastructure Protection http://www.isaccouncil.org/images/ISAC_Role_in_CIP.pdf
- Verizon Data Breaches Investigations Report (2012) http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

Legislation

- The 1996 Clinger-Cohen Act, also known as the Information Technology Management Reform Act (ITMRA), 40 U.S.C. 1401 et seq. https://dodcio.defense.gov/Portals/0/Documents/ciodesrefvolone.pdf
- The 2002 Federal Information Security Management Act (FISMA) 44 U.S.C. § 3541, et seq.)
  - i. https://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf
  - ii. https://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act
- The 2014 Federal Information Security Modernization Act (FISMA 2014) https://www.dhs.gov/fisma
- The National Cybersecurity Protection Act of 2014 https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf
- The Federal Information Technology Acquisition Reform Act (FITARA) of 2014
  - i. https://www.congress.gov/113/plaws/publ291/PLAW-113publ291.pdf#page=148%5D
  - ii. https://management.cio.gov/implementation/
- The Cybersecurity Act of 2015
  - i. https://www.sullcrom.com/siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf
  - ii. https://www.epic.org/privacy/cybersecurity/Cybersecruity-Act-of-2015.pdf
- Robert T. Stafford Disaster Relief and Emergency Assistance Act http://www.fema.gov/media-library-data/1383153669955-21f970b19e8eaa67087b7da9f4af706e/stafford_act_booklet_042213_508e.pdf
- Revised Code of Washington, Chapter 42.56: Public Records Act http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56
  - i. RCW 42.56.590 - Personal information—Notice of security breaches
  - ii. RCW 43.43.856 - Divulging investigative information prohibited—Confidentiality—Security of records and file

APPENDIX I CYBER RESOURCE COMPENDIUM

View with active links:
https://www.dhs.gov/sites/default/files/publications/SLTTGCC%20Cyber%20Resource%20Compendium%202017%2009%2014.pdf

State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC)

Cyber Resource Compendium

This Compendium lists some of the major references that can help build or strengthen an organization's cybersecurity program. There are many other important resources that may not be listed herein. Additionally, each State in the Nation has security reference material and support services that are not listed in this Compendium but will have valuable information that can support a cybersecurity program.

This Compendium will be updated as necessary and republished on a six month cycle. For additional information, contact SLTTGCC@hq.dhs.gov or visit www.dhs.gov/sltt-gcc.

Organization	Free Services	At Cost Services
Multi-State Information Sharing & Analysis Center MS-ISAC (Center for Internet Security)	24x7 Incident Response Cyber Hygiene Kit Nationwide Cyber Sec Review Daily/Weekly Threat Advisories Training Webcasts Patch Advisories Monthly Newsletters Security Primers Daily Tips Feeds Intel and White Papers Malicious Code Analysis Discounted purchasing via Trusted Purchasing Alliance National Cybersecurity Awareness Month Support Stop, Think and Connect Campaign Situational Awareness Reports	Vulnerability Mgmt. Pen Testing Log Analysis Vulnerability Assessments Netflow Monitoring "Albert" Rapid Sensor Deployment Computer Forensics Network Forensics On-site Incident Response Network Monitoring Services Research and Analysis
Critical Infrastructure Cyber Community Voluntary Program, a.k.a. "C3VP," "C-Cubed"	Voluntary Program NIST Cybersecurity Framework Outreach Programs SLTT Toolkit	Vulnerability Management
Infragard	FBI Support Sharing information Sharing intelligence	
Carnegie Mellon University	Emergency Response Support Podcasts	Training
Center for Internet Security	CIS Critical Security Controls	
Cyber Task Force	Info Sharing with FBI Internet Crime Reports	

DRAFT

SLTTGCC Cyber Resource Compendium

Organization	Free Services	At Cost Services
Electronic Crimes Task Force (ECTF)	All Gov Legal Organization All Gov Law Enforcement Aggressive Attack Invest	
National Data Privacy Day/Cyber Security Alliance	Awareness Support	
Cyber Law Enforcement Organization (CLEO)	Cybercrime Reference Support	
Department of Homeland Security (DHS)	Various Resources (Included in this listing) (multitude of Support Services) Protective Security Advisors	
DHS Critical Infrastructure Sector Partnerships	Various Sectors	
Federal Bureau of Investigation (FBI)	Cyber Crimes Most Wanted Scam Information Cyber Shield Malware Investigator iGuardian	
Federal Trade Commission (FTC)	Scams and Fraud Filings	
High Tech Crime Investigative Associates (HTCIA)	Members Only Cyber crime investigations Training	
International Association of Computer Investigation Spec.	IACIS Volunteer Comp Forensics	
Idaho National Lab (INL)	Free Online SCADA Training	
Information Systems Security Association (ISSA)	Association	Fee Driven
Internet Crime Complaint Center (IC3)	FBI & White Collar Crime units Citizen Complaint Process Scam/Fraud Info Info Collector	

Organization	Free Services	At Cost Services
Identity Theft/Fed Trade Commission Support	ID Theft Support	
International Association of Chiefs of Police (IACP)	Online Enforcement Info	
ISACA	Benchmarks Other support and info	
LooksTooGoodToBeTrue.Com	Run be Law Enforcement Cyber Frauds and Scams	
McAfee Institute		Training and Development
National Association of State Chief Information Officers (NASCIO)	Cybersecurity Awareness Resource Guide CISO Toolkit Collaboration Information Exchange Support Cybersecurity Awareness Publications	
National Computer Forensics Institute (NFCI)	Secret Service Run Free for Law Enforcement	
National Criminal Justice Training Center (NCJTC)	Training Technical Assistance	
National Cyber Security Alliance	Safe Online	
National Fusion Center Alliance	Members only Cyber threat intel	
National Governors Association	Resource Center for State Cybersecurity Federal Cybersecurity Programs: A Resource Guide	
National Regional Computer Forensics Lab (RCFL)	Full Services Lab Training	
National White Collar Crime Center	Membership Collaboration	Training
OnGuard Online	Safe Online	
Open Web Application Security Project (OWASP)	References Training	

DRAFT

SLTTGCC Cyber Resource Compendium

Organization	Free Services	At Cost Services
Research and Education Network (REN-ISAC)	Weekly Training Lists	
SANS Institute	Research Training	Training
Texas Engineering Extension Service (TEEX)	Supported by DHS Various Courses	
US-CERT (Computer Emergency Readiness Team)	Support Reference Material Training ICS-CERT Seven Steps to Effectively Defend Industrial Control Systems Labs Support	
Global Cyber Alliance	DMARC-E-mail Authentication DNS Protection Infrastructure	
National Security Agency	Various Resources and Support	
Director of National Intelligence	Coalition of 17 agencies and organizations- Resource	

Additional Tools,Training and Awareness	Type/Level Of Effort	Links
FEMA Training (Various)	Continuity (Multi) /LOW ($0)	https://training.fema.gov/EMIWeb/COOP/
MS-ISAC (msisac.org)	General Awareness /LOW	http://msisac.cisecurity.org/
Center for Internet Security cisecurity.org	General Awareness /LOW	http://alliance.cisecurity.org/
MS-ISAC Cyber Security Advisories	Privacy/Security Staff /LOW	https://msisac.cisecurity.org/advisories/
MS-ISAC Cyber Security Tips Newsletter	General Awareness /LOW	https://msisac.cisecurity.org/newsletters/
MS-ISAC National Webcasts	Privacy/Security Staff /LOW	https://msisac.cisecurity.org/webcast/
IAPP Web Site-Training/White Papers	Privacy/Security Staff LOW/MED	https://www.privacyassociation.org/publications/

No-charge Training and Webcasts- MS-ISAC	ALL /LOW	https://msisac.cisecurity.org/resources/videos/free-training.cfm
Privacy and Security Podcasts Carnegie Mellon		http://www.cert.org/podcasts/
Additional Tools,Training and Awareness	**Type/Level Of Effort**	**Links**
Privacy and Security- Online Training DHS		http://teex.com/teex.cfm?pageid=NERRTCprog&area=NERRTC&templateid=1856
DHS Awareness Training On-line		http://teex.org/teex.cfm?pageid=training&area=teex&Division=KE&Course=AWR136&templateid=14&navdiv=KE
On-line Training Cyber Security Exercise Training		http://teex.org/teex.cfm?pageid=training&area=teex&Division=KE&Course=MGT385&templateid=14&navdiv=KE
Privacy & Security Podcasts (various) US CERT		http://www.cert.org/podcasts/
Privacy & Security Podcasts (various) SANS (no charge)		https://www.sans.org/webcasts/archive/2014
NYU School of Law: Center on Law and Security		http://www.lawandsecurity.org/Portals/0/Documents/Cybersecurity.Partnerships.pdf
CIS Trusted Purchasing Alliance	*Various*	http://alliance.cisecurity.org
SANS Securing The Human	User oriented training /MED	http://alliance.cisecurity.org/opportunity/sans-securing-the-human-purchasing-opportunity.cfm
SANS Technical Training	Privacy/Security Staff /MED	http://alliance.cisecurity.org/opportunity/sans-training.cfm
SANS Securing the Human for Developers	Privacy/Security Staff /MED	http://alliance.cisecurity.org/opportunity/sans-securing-the-human-purchasing-opportunity.cfm
SANS Securing the Human for Utilities	Special/Privacy and Security Staff /MED	http://alliance.cisecurity.org/opportunity/sans-securing-the-human-for-utilities.cfm
SANS Securing the Human Phishing	User oriented training /MED	http://alliance.cisecurity.org/opportunity/sans-securing-the-human-phishing-opportunity.cfm
Software Engineering Institute	Privacy and Security Staff /MED	http://alliance.cisecurity.org/opportunity/sei-cert-stepfwd-opportunity.cfm
(ISC)2 Security Professional Training	Privacy and Security Staff /MED	http://alliance.cisecurity.org/opportunity/isc2-purchasing-opportunity.cfm
Inspired eLearning -- Security and Privacy Awareness Training	General Awareness /MED	http://alliance.cisecurity.org/opportunity/inspired-elearning.cfm
NYU Polytechnic School of Engineering Online Courses	Privacy/Security Staff /MED	http://alliance.cisecurity.org/opportunity/nyu-poly-purchasing-opportunity.cfm

Michigan Cyber Range - Cybersecurity Training and Secure Sandbox	Privacy/Security Staff /MED	http://alliance.cisecurity.org/opportunity/michigan-cyber-range2.cfm
NICCS US-CERT	Formal Security Training	https://niccs.us-cert.gov/formal-education
All State Web Sites	Offer security help and training	Please link to your specific state website

APPENDIX J CYBERSECURITY TRAINING

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT

- ICS-CERT offers 'no-cost' online training https://ics-cert-training.inl.gov/learn
  - Operational Security (OPSEC) for Control Systems (100W) - 1 hour
  - Differences in Deployments of ICS (210W-1) – 1.5 hours
  - Influence of Common IT Components on ICS (210W-2) – 1.5 hours
  - Common ICS Components (210W-3) – 1.5 hours
  - Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
  - Cybersecurity Risk (210W-5) – 1.5 hours
  - Current Trends (Threat) (210W-6) – 1.5 hours
  - Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
  - Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
  - Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
  - Mapping IT Defense-in-Depth Security Solutions to ICS (210W-10) – 1.5 hours
- As well as residential courses that can be hosted by your agency.
  - Introduction to Control Systems Cybersecurity (101) - 8 hrs
  - Intermediate Cybersecurity for Industrial Control Systems (201) - 8 hrs
  - Intermediate Cybersecurity for Industrial Control Systems (202) - 8 hrs
  - ICS Cybersecurity (301) - 5 days

Texas A&M Engineering Extension Service (TEEX) is a founding member of the National Cybersecurity Preparedness Consortium and partners with the federal government to provide 'no cost' training. The web-based courses are offered through three discipline-specific tracks: general, non-technical computer users; technical IT professionals; and business managers and professionals:
https://teex.org/Pages/Program.aspx?catID=607&courseTitle=Cybersecurity
Courses run 2 - 10-hours in length with CEU/CPE hours earned.

Cybrary also offers CEU/CPE hours and certificates of completion. You can search by type, level, or by vendor (left screen). 'No-cost' courses run anywhere from 1 to 43 hours, and there are also options pay a nominal fee for hands-on practice labs, skill assessment, and certification: https://www.cybrary.it/catalog/ It looks geared more towards developing technical career skills, but there are a few good "Beginner"-level courses such as:

- Social Engineering & Manipulation
- Risk Management Framework
- Corporate Cybersecurity Management
- Intro to Cyber Threat Intelligence
- Multiple, 1-hour 'End User' topics
- Multiple, 1-hour 'Fundamentals' topics
- Policy Development
- Business Continuity & Disaster Recovery Planning

Idaho National Laboratory (INL) hosts a five-day ICS Cybersecurity course every year. The course is at an advanced-level and a government-sponsored Industrial Control Systems – U.S. Computer Emergency Response Team (ICS-CERT) program.

The program includes three days of briefings and hands-on classroom training from the Department of Homeland Security's ICS-CERT and INL instructors. This is followed by an eight-hour exercise in which participants are either attacking (red team) or defending (blue team) the INL's chemical process. To learn more, visit https://www.inl.gov/research-programs/control-systems-cyber-security/

SANS Institute – Cybersecurity and Information Security Training https://www.sans.org/

SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center.

SANS provides intensive, immersion training designed to help you and your staff master the practical steps necessary for defending systems and networks against the most dangerous threats - the ones being actively exploited. The courses are full of important and immediately useful techniques that you can put to work as soon as you return to your offices. They were developed through a consensus process involving hundreds of administrators, security managers, and information security professionals, and address both security fundamentals and awareness, and the in-depth technical aspects of the most crucial areas of IT security.

Institute for Cybersecurity – Law Enforcement Specific

The National Sheriffs' Association, Global Center for Public Safety has created the Institute for Cybersecurity. Training courses and certifications have been designed specifically for law enforcement to arm them with the understanding and knowledge they need to, not only conduct criminal investigations and develop intelligence, but to provide meaningful information to those they serve. These are not forensics or technical courses, rather, they provide the operational knowledge and understanding for all members of law enforcement, from the Sheriff to the newest dispatcher.

Courses are taught in 2-hour, 4-hour or 8-hour blocks of instruction and can be adjusted to meet the needs of a particular department or law enforcement officer.

All courses are currently being taught face-to face by subject matter experts, most of whom have a law enforcement background, traveling to your agency.

COURSES:

- Introduction to Cybersecurity
- Social Media for Law Enforcement
- Fundamentals of Ransomware
- Understanding Crypto Currency
- The Dark Web
- Law Enforcement and the Fusion Center

Additionally, a 40-hour certification course is being offered in Cyber Intelligence. The course will be designed for the more in-depth study of cyber intelligence analysis including how to develop information into meaningful intelligence which is critical to the planning, intelligence, and investigative activities of a law enforcement agency. The course is designed to assist law enforcement officers in obtaining the knowledge, skills and abilities that they require to further their careers in law enforcement.

For course pricing and discount opportunities for your organization, please email: cyber@globalhomeland.org.