



# **CHARTER**

for the

Region 5 Cyber Planning Team

Adopted September 27, 2018

## Charter Contents

Introduction .....	3
Region 5 Cyber Planning Team Strategy .....	3
Cyber Planning Team .....	3
Purpose .....	3
Program Components .....	3
Goals .....	4
Outcomes .....	4
Deliverables .....	4
Timeline .....	5
Authorities.....	6
Roles and Responsibilities .....	6
Conflict of Interest .....	10
Changes and Amendments .....	11
Appendix A: List of Representatives .....	12
Appendix B: Cybersecurity Function of the Incident Command System .....	13
Appendix C: Cyber Incident Response Team Position Qualifications .....	15
Appendix D: FEMA Cybersecurity Resource Typing Definition.....	20

## **Introduction**

The purpose of the Cyber Planning Team (CPT) is to provide guidance and recommendations to all disciplines and sectors within Region 5 (Tacoma-Pierce County) to prevent, protect against, respond to, recover from, and mitigate against acts of terrorism and other technological and human-caused events conducted through cyberspace. Guidance and recommendations will be in the form of planning, training, and exercises.

The initial campaign will be conducted over a period of 12 months, at the end of which the CPT will evolve into a Cyber Advisory Group for the Region.

This charter outlines the Region 5 CPT Purpose, Strategy, Goals, Outcomes, Deliverables, and Components. The intention of this charter is to provide direction and clear goal setting of the CPT campaign and programs, and highlights agencies roles and responsibilities, to include the role of Cyber Incident Response Team (CIRT).

## **Strategy**

Public and private organizations across Region 5 are entrusted with sensitive and confidential information that include, but not limited to, Criminal Justice Information (CJI), Protected Health Information (PHI), Federal Tax Information (FTI), and Personally Identifiable Information (PII). Pierce County has established a regional Cyber Planning Team Strategy intended to align information security with operational strategy; to comply with applicable legal and regulatory requirements; to achieve industry standards; to manage, monitor, and mitigate information security risks and incidents; to optimize information security investments; to manage information security resources efficiently; and to monitor the ongoing effectiveness of the Cyber Planning Team campaign and subsequent programs.

## **Campaign and Programs**

### Program Components

#### Information Risk Management

Identify and manage information security risks and align the Strategy with the operational needs of County organizations.

#### Program Development

Create and maintain a program to implement the Strategy.

#### Incident Management & Response

Plan, develop, and manage appropriate capabilities and measures to detect, respond to, and recover from information security incidents.

#### Governance

Establish and maintain a governance structure through the CPT to provide for accountability and assurance that the Strategy is aligned with the operational needs of County agencies and consistent with applicable law, regulations, and industry best practices.

## Region 5 Cyber Planning Team Charter

Costs—hiring positions, including an expert consultant, security software, mitigation—will fall under each agency’s discretion as allowable for the time being. Grant funding *is* an option, and a process will be established by the Region 5 Cyber Advisory Group once it transitions from being the Cyber Planning Team.

CPT membership and governance may evolve over time, as appropriate, to support sustainment of continued dialogue on cyber planning.

### Goals (derived from CPT survey)

- Promote and enhance collaboration on strategies and policies to address cybersecurity
- Conduct agency-specific Business Impact Analysis (BIA)
- Develop organizational Continuity of Operations (COOP)/Business Continuity Planning
- Improve technical-to-end-user information sharing
- Develop a framework for understanding regulatory requirements
- Develop a multi-year, progressive training and exercise plan across each organization that includes key stakeholders
- Build and strengthen partnerships between local, county, state, federal, and private sector partners
- Encourage networking among public and private sector stakeholders to identify interdependencies before a disaster
- Develop a system/schedule to socialize Suspicious Activity Reporting (SAR) procedures to all levels of employees
- Leadership buy-in of the cybersecurity philosophy to promote organizational security awareness
- Enhance resiliency to cybersecurity incidents through discussion of cyber incident reporting, protocols, and available regional resources
- Prioritize the training needed to implement regional plans and polices
- Prioritize training needed to support regional exercises
- Prioritize regional exercises that build or sustain capabilities

### Outcomes

- Policies and procedures for internal and external reporting
- Methods for the lateral sharing of cyber-specific intelligence between Region 5 disciplines
- Develop a process that supports deployment of regional and state incident response teams
- Robust understanding of situational awareness, trends, tactics, procedures (*US-CERT alerts*)
- Quarterly, recommended list of situational awareness resources and recommendations
- More efficient operational coordination amongst the region
- Create/develop understanding of ‘common terminology’ between end-user, EM, and IT; vs plain language.

## Deliverables

- A regional Concept of Operations (CONOPS) that identifies triggers for:
  - ✓ WHEN to report both internally and externally,
  - ✓ WHO to report to both internally and externally—while acknowledging specific federal, state, and local regulatory reporting requirements—
  - ✓ Consistent throughout Region 5 (Tacoma-Pierce County).
- A comprehensive regional training and exercise resource collection.
- A regional cyber advisory board.
- A Cyber Incident Response Team (CIRT) capable of at least local response; with the intent of intra- and inter-state response (pending legislature).

## Project Timeline

The team will meet monthly to discuss assignments, verify task completion, and track project progress as it relates to identified milestone deadlines, with breakout work to be completed between meetings.

- RCC Meeting Project Introduction and Approval February 2018
- Select Project Team Members February 2018
- Conduct Organizational Cyber Survey February 2018
- Project Introduction to CPT March 2018
- Develop Strategic Plan March 2018
- Review/Vet Current Regional Priorities / Goals March 2018
- Develop Project Charter with Timeline March 2018
- Focus: Intelligence and Information Sharing April 2018
- Develop Response Plans April 2018
- Focus: Business Continuity/Continuity of Operations May 2018
- Develop Recovery Plans May 2018
- Present Vision / Mission / Values to RCC June 2018
- Conduct At-Will Cyber Tabletop Exercise (TTX) Via Home Agency June 2018
- Debrief Agency-Specific TTX From June August 2018
- Review and Adopt CPT Charter August 2018
- Align Applicable State and Federal Regulations to CONCOPS August 2018
- Review/Vet Drafted Response and Recovery Plans August 2018
- Debrief Individual Agencies' Cyber TTX from June August 2018
- Draft and Review V1 CONOPS September 2018
- Present Status and Progress to RCC September 2018
- Conduct a Cyber TTX Group/Regional Exercise October 2018
- Status Check of CIRT Qualifications and Training November 2018
- Develop Next-to-Final Draft of CONOPS January 2019
- Gather Stakeholder / Partner / RCC Feedback February 2018
- Agency Leadership Review of Final CONOPS February 2019
- Regional TTX Facilitated by NCEPP March 2019
- Publish Final CONOPS and Present to RCC April 2019
- Celebrate! April 2019

## Authority

### Compliance

Each agency is responsible for ensuring they met any regulatory compliance such as Payment Card Industry Data Security Standards (PCI DSS), NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection), and or Health Insurance Portability and Accountability Act (HIPAA). This includes completing the required forms and assessment.

The assigned agency technology representative oversees the security policies, standards, guidelines, processes, and procedures. It is important that the representative establish cooperative relationships with management, data owners, data custodians, and information users.

Responsibilities include, but are not limited to:

- Review existing internal controls in place to monitor and report exceptions or violations and prepare reports of findings;
- Recommend improvements or oversee the development of controls necessary to monitor compliance;
- Review reports of technical violations or alerts that are recorded in logs to ensure they are appropriately addressed;
- Review and report how incidents or threats (such as unauthorized access, misuse, modification, duplication, or disclosure of information) are handled and controlled for compliance; and,
- Review the reporting compliance requirements and ensure they are met.

**Membership:** The CPT brings together subject matter experts that represent each discipline of county functionality and considers whole community interdependencies. To the extent practicable, the membership will be geographically and professionally diverse. Members are expected to participate in the development and implementation of CPT goals and objectives; participate in CPT meetings and the appropriate sub-groups tasked with certain deliverables; coordinate with other stakeholders in the region/agency the member represents; and engage in planning activities, surveys, and product review as necessary.

### Representation

Representatives shall be appointed by their designated agencies and confirmed by the CPT Chair/Campaign Driver. Members may invite advisory participants to assist the Team. The 12-month initial campaign length negates the need for elections and term limits. Leadership will be revisited once the campaign transitions to an advisory board.

The CPT representatives shall include up to two (2) individuals—end-user and IT Security—from each of the following agencies/groups:

Critical Infrastructure: Private *and* Public Sectors  
Cities & Towns

## Region 5 Cyber Planning Team Charter

Fire Chief's Association  
Higher Education Representative  
Hospitals: CHI Franciscan Health System, MultiCare Health System  
Pierce County Emergency Management  
Pierce County Information Technology  
Pierce County Police Chiefs Association  
Pierce County Sheriff's Department  
Port of Tacoma  
Public Safety Answering Points (PSAPs)  
Puyallup Tribe  
School Districts, K-12  
Tacoma Fire Department  
Tacoma-Pierce County Health Department  
Tacoma Police Department  
Transportation

### **Roles and Responsibilities**

Program Oversight of the CPT is performed by Pierce County Emergency Management.

Program Management of the CIRT is performed by the Pierce County Information Technology Department, with program oversight performed by Pierce County Emergency Management.

It is essential to the success of this project that the Team be committed to accomplishing the stated purpose and outcomes for this project. To accomplish this, the Team is resolved to take the following active roles and responsibilities.

- Participate fully in Team meetings.
- Share knowledge and expertise for the benefit of the Team and the accomplishment of the study.
- Be willing to explore creative “outside the box” solutions.
- Accomplish “homework” at appropriate times to support the accomplishment of the project.
- Contribute to project completion report.
- Work collectively toward accomplishing the study purpose.

### Information Technology Security Officer (ITSO), agency-specific

The ITSO is responsible for the development, maintenance, and implementation of the Information Security Program. The ITSO works with the Cyber Incident Response Team (CIRT) and works with various county offices, Agencies, vendors, assurance functions, and internal or external parties to implement, monitor, and execute the program. The core responsibilities of each agency's ITSO are:

## Region 5 Cyber Planning Team Charter

### Governance

- Develop, oversee, implement, and maintain the Cyber Planning Team Strategy and related initiatives at an agency-level.
- Align the CONCOPS with their agency operational strategy.
- Liaise with agency leadership and process owners to support ongoing alignment, verify risk and operational impact assessments are conducted, and that risk mitigation strategies are being implemented.
- Assist in identifying current and potential legislation and regulatory requirements affecting information security.
- Monitor utilization and effectiveness of information security resources by developing and implementing monitoring and metrics.
- Liaise with other assurance providers (e.g., Audit, Compliance, Privacy, etc.) regarding information security.
- Provide assurance for proper response and reporting of information security incidents.
- Define agency-specific information security roles and responsibilities, consistent across discipline and or Region.
- Establish reporting and communication needed to support the CONOPS.
- Assure through policy the appropriate use of the agency's information resources.
- Educate employees about their information security and privacy protection responsibilities.

### Information Risk Management

- Establish and maintain processes for information asset classification and ownership.
- Implement a systematic and structured information risk assessment process.
- Confirm operational impact assessments are conducted periodically.
- Verify threat and vulnerability evaluations are performed on an ongoing basis.
- Identify and periodically evaluate information security controls and countermeasures for mitigation of risk to acceptable levels.
- Integrate risk, threat, and vulnerability management into operational life cycle processes (e.g., project management, development, procurement, and employment life cycles).
- Report significant changes in information security risk to appropriate levels of management on both periodic and incident-driven basis.

### Program Development and Management

- Develop, maintain, and manage plans to implement the CPT Strategy while providing clear visibility to the specific activities being performed within the CONOPS.
- Establish, communicate, and maintain information security policies, and verify that processes and procedures are performed in a compliant manner.
- Confirm the development, communication, and maintenance of standards, procedures, and other documentation (e.g., guidelines, baselines, codes of conduct) that support information security policies.
- Develop the information security resources, including people, processes, and technology.

## Region 5 Cyber Planning Team Charter

- When applicable, working with agency leadership, identify and manage internal and external resources (e.g., finances, people, equipment, systems) required for the execution of the program.
- Develop processes to ensure applicable contracts and agreements contain the necessary information security controls (e.g., outsourced providers, residents, third parties).
- Provide CONOPS advice and guidance (e.g., risk and analysis, control options) to the home agency, discipline, and Region.
- Ensure alignment between the CONOPS and other assurance functions.
- Design, develop, and manage processes to provide information security awareness, training, and education to the appropriate audiences. (e.g., process owners, users).
- Define and establish metrics to evaluate the effectiveness of the CONOPS.
- Verify any CONOPS compliance issue or other variance is addressed with the CPT a timely manner.
- Monitor, measure, validate, and report on the effectiveness and efficiency of information security controls and program compliance.

### Incident Management and Response

- Develop and implement processes to prevent, detect, respond, and recover from information security incidents.
- Establish clear escalation and communication processes including lines of authority during incident response.
- Develop and maintain incident response plans to ensure timely response, reporting, and remediation.
- Establish the capability to investigate and analyze information security incidents to determine root cause (e.g., forensics, evidence collection and preservation, log analysis, interviewing).
- Develop a process in accordance with Incident Management & Response Policy to communicate with internal parties and external organizations (e.g., media, law enforcement, residents).
- Integrate information security incident response plans with the Region's disaster recovery and operational continuity plans.
- Periodically test and refine information security incident response plans.
- Manage the response to information security incidents.
- As needed, conduct reviews of systems, applications, networks, or processes related to previous information security incidents to ensure remediation actions are working as designed.
- Develop corrective actions, reassess risk, and establish monitoring mechanisms as needed.

### Region 5 Cyber Incident Response Team (CIRT)

The CIRT will be comprised of specific Region 5 IT resources at various operational levels with the primary responsibility of performing operational information security functions, based from the FEMA typing in Appendices C & D. Members will be vetted by PCEM for Emergency Worker certification and fundamental ICS training, and by PCIT for position-specific training. Lead by

## Region 5 Cyber Planning Team Charter

PCIT, the CIRT works with applicable Pierce County Agency resources to develop, implement, communicate, and apply the CONOPS to Region 5 as allowable.

The core responsibilities of the CIRT are:

- Provide guidance, support, and direction for all information security activities for the Region in accordance with and in support of the Region 5 CONOPS.
- Provide direction for all information security response activities for the Region in accordance with and in support of the CONOPS.
- Engage and work with various Regional agencies, offices, assurance functions, and internal and external parties as needed for managing the program.
- Take appropriate steps and actions for managing and responding to information security incidents, policy violations, forensics and investigations, internal or external exploits, threats and vulnerabilities.
- Provide Incident Command System (ICS) direction in line with operational goals and objectives and relevant laws and regulations, demonstrate support for, and commitment to information through the maintenance and implementation of the CONOPS across the Region.

### **Conflict of Interest**

The intention of this “Conflict of Interest” article is to remind all CPT representatives that the primary objective of the CPT is to reach decisions that strengthen the ability of the Region to respond to all hazard incidents. To achieve this intention, all representatives agree to place regionwide benefit above personal and or single agency benefit.

CPT representatives from government organizations shall be subject to the code of ethics for their respective jurisdiction/agency. See also Chapter 42.23 RCW (Code of Ethics for Municipal Officers).

In the event any non-governmental individuals or organizations are appointed as representatives on the CPT, such individuals or organizations shall not be beneficially interested, directly or indirectly, in any contract which may be made by, through or under the supervision of such representative or organization, in whole or in part, or which may be made for the benefit of his or her office or organization or accept, directly or indirectly, any compensation, gratuity or reward in connection with such contract from any other person beneficially interested therein.

Any non-governmental CPT representative or organization that could potentially be beneficially interested, directly or indirectly, in any contract in conflict with this Article shall inform the team before participating in a discussion.

**Changes and Amendments**

Changes and Amendments to this Charter may be proposed by any member of the CPT. The CPT will review and approve the proposed changes or amendments.

Record of Changes

Change Number	Location of Change	Date of Change	Individual Making Change	Description of Change

## Appendix A: CPT Representatives

<b>Jurisdiction/Agency</b>	<b>Primary</b>	<b>Alternate(s)</b>
Cities & Towns (City of Puyallup)	Clay Doolittle (IT)	Jill McNally
Fire Chiefs		
Higher Education	Pat Taylor	Oka Keiji
Hospitals	Eileen Newton	
Pierce County Emergency Management	Natalie Stice	
Pierce County Information Technology	Russ Tena	
Pierce County Sheriff's Department	Brent Van Dyke (IT)	
Pierce County Utilities	Gloria Van Spanckeren	Don Rennie (IT)
Police Chiefs		
Port of Tacoma	Marty Kapsh	Paul Adams (IT)
Private Utilities	Nick Foster (IT)	Jeff Custer (IT)
Tacoma Public Utilities	Matt Beaumont (IT)	
Private Consultants	Hillman Mitchell	David Shaw
Public Safety Answering Points (PSAP)	Wesley Strauss (IT)	Jonathan Brock (IT)
Puyallup Tribe	Larry Mauritson	
School Districts (K-12)	Katie Gillespie	Liza Klumpar (IT)
Tacoma Fire Department	Ute Weber	
Tacoma-Pierce County Health Department	Brien Aguilar (IT)	
Tacoma Police Department		
State Emergency Management	Robert Lang	Alisha King (WaTech)
DHS/FEMA	Dana Lockhart	Barrett Adams-Simmons

### **CPT Leadership**

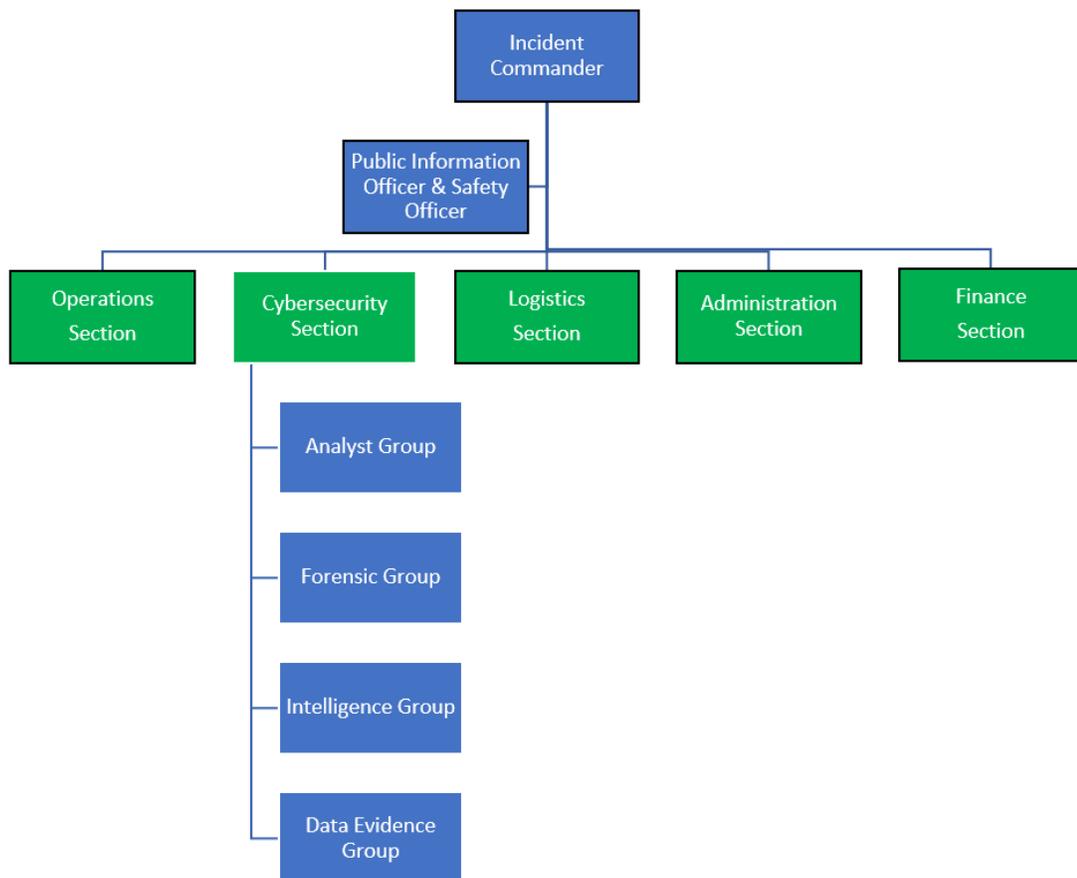
Chair: Natalie Stice

Vice-Chair:

## Appendix B: Cybersecurity Function of the Incident Command System

NIMS's scalability and flexibility allow for a cybersecurity function to be integrated into the ICS. The cybersecurity function permits for the investigation, information collection, analysis, and sharing of data that could identify the origin of a cyber incident or attack. If the emergency or incident was determined to be the result of a cyber-attack, the cybersecurity function would lead the investigation and operational response. If the cyberattack was determined to be a criminal act, the cybersecurity function would share the information with the proper operational enforcement authorities.

The cybersecurity function should be installed in the general staff section of the ICS when a critical infrastructure system is associated with an incident as shown below. The function may be combined with other general staff sections to form task force operations to understand the nature of the incident further, share information and ensure primary response objectives are completed.



**Analyst group:** Provide tactical and strategic level analysis of cyber threats, vectors, and actors supporting the defense of computer network operations.

**Forensic group:** Provide forensic analysis of computer network operations to investigate data, preserve malicious data as evidence, and determine routes of the system or network entry.

## Region 5 Cyber Planning Team Charter

**Intelligence group:** Monitor computer network systems and other data sources to predict nefarious cyber actor behaviors, determine if threats are credible, share information with other organizations, and develop situation reports.

**Data evidence group:** Manage preserved data evidence and share it with agencies or organizations for future criminal prosecution.

## Appendix C: Cyber Incident Response Team Position Qualifications

The Emergency Worker Program is a volunteer oriented program established by RCW 38.52.310. Emergency workers are provided liability, medical, and personal property coverage as well as reimbursement for some incidental expenses while deployed on state-approved incidents and training events.

Washington Administrative Code (WAC) 118-04 implements the provisions of RCW 38.52 by establishing the procedures and qualifications for registration of "emergency workers" (volunteers) and explains how the compensation program is administered. Any Claimant for compensation must have been working under Emergency Management authority at the time of the accident. A state Mission number or Training Mission number must have been assigned.

In accordance with RCW 38.52.030(3), 38.52.070(1), and 38.52.400(1), the incident command system shall be used for all multiagency/multijurisdiction operations.

The following are criteria for completion in order to be eligible for emergency worker status:

- ✓ FEMA IS-100: Introduction to the Incident Command System, ICS 100
- ✓ FEMA IS-700: Introduction to the National Incident Management System
- ✓ FEMA IS-800: Introduction to the National Response Framework
- ✓ FEMA IS-200: Incident Command System for Single Resources and Initial Action Incidents
- ✓ Pierce County Sheriff's Department Background Check

Online training resources: <https://training.fema.gov/nims/>

Local training resources: <http://www.co.pierce.wa.us/2987/Training>

### FEMA Typing Library – Position Qualifications

#### ***Adopted by Pierce County and Washington State***

<https://rtlt.preptoolkit.fema.gov/Public/Combined?s=&a=&q=cyber>

- 13-509-1252 Computer Network Defense Infrastructure Support Specialist
- 13-509-1251 Computer Network Defense Analyst
- 13-509-1250 Cyber Incident Responder (*listed below*)
- 13-509-1254 Data Administration Specialist
- 13-509-1253 Digital Forensics Specialist
- 13-509-1248 Supervisory Control and Data Acquisition Controller Specialist
- 13-509-1249 Supervisory Control and Data Acquisition Server Specialist

**CYBER INCIDENT RESPONDER**

TYPE	TYPE 1	TYPE 2
<b>DESCRIPTION</b>	The NIMS Type 1 Cyber Incident Responder: 1. Serves as the team leader on the Cyber Incident Response Team 2. Responds to crisis or urgent situations aimed at mitigating, preparing for, responding to, and recovering systems from cyber threats 3. Completes cyber incident response reports during and after deployments	The National Incident Management System (NIMS) Type 2 Cyber Incident Responder: 1. Works under the technical direction of a NIMS Type 1 Cyber Incident Responder aimed at mitigating, preparing for, responding to, and recovering systems from cyber threats 2. Responds by completing actions that are crucial to prevent loss of life, preserve property, and secure information while investigating and analyzing all relevant response activities 3. Supports the NIMS Type 1 Cyber Incident Responder by preparing reports during and after deployments, which include all actions taken to properly document a cyber incident during the operation
<b>CATEGORY</b>	<b>CRITERIA</b>	<b>CRITERIA</b>
<b>EDUCATION</b>	Not Specified	Not Specified
	<b>NOTES:</b> Not Specified	
<b>TRAINING</b>	Same as Type 2	Completion of the following: 1. IS-100: Introduction to Incident Command System, ICS-100 2. IS-200: Incident Command System for Single Resources and Initial Action Incidents 3. IS-700: National Incident Management System, An Introduction 4. IS-800: National Response Framework, An Introduction 5. IS-860: National Infrastructure Protection Plan, An Introduction 6. Agency Having Jurisdiction (AHJ)-determined cyber forensics training
	<b>NOTES:</b> Any use of the term "forensics" is descriptive of a skill or capability and does not imply a law enforcement role.	



TYPE	TYPE 1	TYPE 2
<p><b>EXPERIENCE</b></p>	<p>Same as Type 2, PLUS: Knowledge, Skills, and Abilities:</p> <ol style="list-style-type: none"> <li>1. Writing technical reports that describe the exploited vulnerability, the applied security control(s) to correct the immediate problem, and any recommended additional controls or changes in process or policy</li> <li>2. Writing executive-level reports and presentations to communicate the cause of the exploited vulnerability, the applied security control(s) to correct the immediate problem, and any recommended additional controls or changes in process or policy with senior leaders</li> </ol> <p>AHJ-documented and validated experience demonstrated in the following areas:</p> <ol style="list-style-type: none"> <li>1. Coordinating with and providing expert technical support to enterprise-wide CND specialists to resolve CND incidents</li> <li>2. Performing in command and control functions in response to incidents</li> <li>3. Identifying and assessing the capabilities and activities of cyber criminals or foreign intelligence entities</li> </ol>	<p>AHJ-documented and validated knowledge, skills, and abilities demonstrated in the following areas:</p> <ol style="list-style-type: none"> <li>1. Data backup, types of backups, and recovery concepts and tools</li> <li>2. How network services and protocols interact to provide network communications</li> <li>3. Evidence recovery techniques and the use of the corresponding industry tools</li> <li>4. Log data analytics and the use of the corresponding industry tools</li> <li>5. Incident categories, incident responses, and timelines for responses</li> <li>6. Cyber incident response and handling methodologies</li> <li>7. Intrusion detection methodologies and techniques for detecting host- and network-based intrusions</li> <li>8. Network protocols and directory services</li> <li>9. Network traffic analysis methods</li> <li>10. Packet-level analysis</li> <li>11. System and application security, network attacks as related to threats and vulnerabilities</li> <li>12. Cybersecurity event correlation tools</li> <li>13. Computer network defense (CND) policies, procedures, and regulations</li> <li>14. Different classes of cyber attacks</li> <li>15. Different operational cyber threat environments</li> <li>16. Malware analysis and handling, network protection against malware</li> <li>17. Basic system administration, network, and operating system hardening techniques</li> <li>18. General cyber-attack stages</li> <li>19. Attack source profiling techniques</li> <li>20. Network security architecture concepts, including topology, protocols, components, and principles</li> <li>21. Preserving evidence integrity according to standard operating procedures or national standards</li> <li>22. Securing network communications</li> <li>23. Recognizing and categorizing types of vulnerabilities and associated attacks</li> <li>24. Performing damage assessments</li> <li>25. Writing technical reports about exploitation and mitigation</li> </ol> <p>AHJ-documented and validated experience demonstrated in the following areas:</p> <ol style="list-style-type: none"> <li>1. Evidence recovery techniques and the use of the corresponding</li> </ol> <p>(Continued)</p>

	Position Qualifications for Cybersecurity Cybersecurity	Federal Emergency Management Agency
---	--	-------------------------------------

TYPE	TYPE 1	TYPE 2
<b>EXPERIENCE</b>		(Continued) industry tools 2. Correlating incident data to identify specific vulnerabilities 3. Determining attack attribution and electronic data collection 4. Monitoring external data sources to maintain currency of the CND threat condition and determine which security issues may have an impact on the enterprise 5. Performing analysis of log files from a variety of sources to identify possible threats to network security 6. Performing CND incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation 7. Performing initial, forensically sound collection of images, logs, and other critical components in order to discern possible mitigation/remediation on enterprise systems 8. Performing real-time CND incident handling tasks as a member of or in support of deployable Incident Response Teams (IRT) 9. Receiving and analyzing network alerts from various sources within the enterprise and determine possible causes of such alerts 10. Tracking and documenting CND incidents from initial detection through final resolution 11. Analyzing collected information to identify vulnerabilities and potential for exploitation 12. Identify weak wireless access points
	<b>NOTES:</b> The knowledge, skills, and abilities align with the National Initiative for Cyber Education (NICE) National Cybersecurity Workforce Framework.	
<b>PHYSICAL/MEDICAL FITNESS</b>	Not Specified	Not Specified
	<b>NOTES:</b> Not Specified	
<b>CURRENCY</b>	Not Applicable	1. Participates in exercise, drill, or simulation at least once every year 2. Background checks as applicable law permits and requires
	<b>NOTES:</b> Provider must carry out and use any background checks as applicable law specifies. This may include a background check completed within past 12 months; sex-offender registry check; and a local, state, and a local, state, and national criminal history.	
<b>PROFESSIONAL AND TECHNICAL LICENSES AND CERTIFICATIONS</b>	Same as Type 2, PLUS: 1. Compliance in one of the following: a. Certified Digital Forensic Examiner (CDFE) b. Certified Computer Crime Investigator (CCCI) 2. Information Assurance Certification 3. Certified Incident Handler	1. Technical qualifications equivalent to Department of Defense Directive (DoDD) 8570 Level 2 (Technical) and compliance in Certified Digital Media Collector (CDMC) 2. Certification in Cyber Forensics
	<b>NOTES:</b> Not Specified	



## ORDERING SPECIFICATIONS OR DESIGNATIONS

---

1. (X) Can be ordered as an individual asset
2. (X) Can be ordered in conjunction with a NIMS typed team (Cyber Incident Response Team)
3. ( ) Can be ordered in conjunction with a NIMS typed unit
4. Discuss logistics for deploying this position, such as security, lodging, transportation, and meals, prior to deployment
5. This position typically works 12 hours per shift, is self-sustainable for 72 hours, and is deployable for up to 14 days

## REFERENCES

---

1. FEMA, NIMS 508: Cyber Incident Response Team
2. U.S. Department of Homeland Security, National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, v.2, May 2014
3. Department of Defense Directive (DoDD), 8570 and Global Information Assurance Certification (GAIC), January 2014

## NOTES

---

Nationally typed resources represent the minimum criteria for the associated category.

## APPENDIX D: FEMA Cybersecurity Resource Typing Definition

 <b>Homeland Security</b>	Resource Typing Definitions for Cybersecurity Cybersecurity	<b>Federal Emergency Management Agency</b>
--	--	--

### CYBER INCIDENT RESPONSE TEAM

<b>DESCRIPTION</b>	The Cyber Incident Response Team responds to crises or urgent situations within the pertinent cyber domain to address, manage, and mitigate immediate and potential threats.		
<b>RESOURCE CATEGORY</b>	Cybersecurity	<b>RESOURCE KIND</b>	Team
<b>OVERALL FUNCTION</b>	The Cyber Incident Response Team: 1. Investigates and analyzes all relevant cyber and network activities related to the crisis situation with the purpose of achieving the speediest recovery of the impacted critical infrastructure service 2. Uses mitigation, preparedness, response, and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security 3. Documents all steps and actions taken during the operations and develops Incident Action Reports (IAR)	<b>COMPOSITION AND ORDERING SPECIFICATIONS</b>	1. Discuss logistics for deploying this team, such as security, lodging, transportation, and meals, prior to deployment 2. This team typically works 12 hours per shift, is self-sustainable for 72 hours, and is deployable for up to 14 days 3. The requestor may need to order multiple teams to provide 24 hour coverage 4. A single source entity may constitute the entire team 5. The requestor should specify if the personnel should have training and experience with specific software applications, hardware, and equipment

RESOURCE TYPES			TYPE 1	NO TYPE 2	NO TYPE 3	NO TYPE 4
COMPONENT	METRIC/ MEASURE	CAPABILITY				
Personnel	Per Team	Minimum	15	Not Applicable	Not Applicable	Not Applicable
<b>NOTES:</b> Not Specified						
Personnel	Per Team	Management and Oversight	2 - National Incident Management System (NIMS) Type 1 Cyber Incident Responder	Not Applicable	Not Applicable	Not Applicable
<b>NOTES:</b> Not Specified						

RESOURCE TYPES			TYPE 1	NO TYPE 2	NO TYPE 3	NO TYPE 4
COMPONENT	METRIC/ MEASURE	CAPABILITY				
Personnel	Per Team	Operations and Support	1 - NIMS Type 2 Cyber Incident Responder 3 - NIMS Type 1 Computer Network Defense (CND) Analyst 1 - NIMS Type 1 CND Infrastructure Support Specialist 1 - NIMS Type 2 CND Infrastructure Support Specialist 1 - NIMS Type 1 Database Administration Specialist 1 - NIMS Type 1 Digital Forensics Specialist 1 - NIMS Type 2 Digital Forensics Specialist 1 - Voice Communications Operator 1 - System Administrator 2 - Network Administrator	Not Applicable	Not Applicable	Not Applicable
			<b>NOTES:</b> 1. All members of the team should hold an active security clearance. 2. Any use of the term "forensics" is descriptive of a skill or capability and does not imply a law enforcement role. 3. The Voice Communications Operator, System Administrator, and Network Administrator are not NIMS typed support positions.			

RESOURCE TYPES			TYPE 1	NO TYPE 2	NO TYPE 3	NO TYPE 4
COMPONENT	METRIC/ MEASURE	CAPABILITY				
Equipment	Per Team	Operations	13 - Laptops with wireless internet card and programs for creation of documents, spreadsheets, and databases 2 - Laptops with a digital forensics tool suite 2 - Write-block hardware devices 2 - Devices capable of live memory capture	Not Applicable	Not Applicable	Not Applicable
			<p><b>NOTES:</b> 1. Team may need additional equipment and supplies for small local area network interfaces to tactical outbound communications. 2. An understanding of asset information including operating systems, key applications, incident response plans, organization charts, emergency contact lists, and hardware is essential prior to deploying team, to ensure team brings the appropriate tools. 3. Iterations of training deployments determine additional software and hardware items to conduct forensics, network analysis, and other supporting functions.</p>			
Equipment	Per Team Member	Communications	1 - Cell phone	Not Applicable	Not Applicable	Not Applicable
			<p><b>NOTES:</b> Consider alternate forms of communication, such as satellite phones, based on the mission assignment and team needs.</p>			

## COMMENTS

---

1. The requestor provides support to the team, such as security, fuel, and power for recharging phones, computers, and other rechargeable devices

## REFERENCES

---

1. FEMA, NIMS 509: CND Analyst
2. FEMA, NIMS 509: CND Infrastructure Support Specialist
3. FEMA, NIMS 509: Cyber Incident Responder
4. FEMA, NIMS 509: Database Administration Specialist
5. FEMA, NIMS 509: Digital Forensic Specialist
6. U.S. Department of Homeland Security, National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, v.2, May 2014

## NOTES

---

Nationally typed resources represent the minimum criteria for the associated component and capability.