

CYBER INCIDENT RESPONDER

RESOURCE CATEGORY	Cybersecurity
RESOURCE KIND	Personnel
OVERALL FUNCTION	The Cyber Incident Responder mitigates, prepares for, responds to, and recovers systems from cyber threats
COMPOSITION AND ORDERING SPECIFICATIONS	<ol style="list-style-type: none"> 1. This position can be ordered as a single resource or in conjunction with a NIMS typed team (Cyber Incident Response Team). 2. Discuss logistics for deploying this position, such as security, lodging, transportation, and meals, prior to deployment 3. This position typically works 12 hours per shift, is self-sustainable for 72 hours, and is deployable for up to 14 days

Each type of resource builds on the qualifications of the type below it. For example, Type 1 qualifications include the qualifications in Type 2, plus an increase in capability. Type 1 is the highest qualification level.

COMPONENT	TYPE 1	TYPE 2	NOTES
DESCRIPTION	<p>The NIMS Type 1 Cyber Incident Responder:</p> <ol style="list-style-type: none"> 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 	<p>The National Incident Management System (NIMS) Type 2 Cyber Incident Responder:</p> <ol style="list-style-type: none"> 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 	Not Specified
EDUCATION	Not Specified	Not Specified	Not Specified
TRAINING	Same as Type 2	<p>Completion of the following:</p> <ol style="list-style-type: none"> 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 	Any use of the term "forensics" is descriptive of a skill or capability and does not imply a law enforcement role.

Superseded

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

Superseded

Position Qualification for Cybersecurity
Cybersecurity

COMPONENT	TYPE 1	TYPE 2	NOTES
EXPERIENCE		<p>(Continued) mitigation</p> <p>AHJ-documented and validated experience demonstrated in the following areas:</p> <ol style="list-style-type: none"> 1. Evidence recovery techniques and the use of the corresponding 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 	
PHYSICAL/MEDICAL FITNESS	Not Specified	Not Specified	Not Specified
CURRENCY	Not Applicable	<ol style="list-style-type: none"> 1. Participates in exercise, drill, or simulation at least once every year 2. Background checks as applicable law permits and requires 	<p>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.</p>

Position Qualification for Cybersecurity
Cybersecurity

COMPONENT	TYPE 1	TYPE 2	NOTES
PROFESSIONAL AND TECHNICAL LICENSES AND CERTIFICATIONS	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	Not Specified

Superseded



Position Qualification for Cybersecurity Cybersecurity

NOTES

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

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

Superseded