COMPUTER NETWORK DEFENSE INFRASTRUCTURE SUPPORT SPECIALIST

RESOURCE CATEGORY	Cybersecurity
RESOURCE KIND	Personnel
OVERALL FUNCTION	The Computer Network Defense (CND) Infrastructure Support Specialist tests, implements, deploys, and administers infrastructure hardware and software to manage network defenses
COMPOSITION AND ORDERING SPECIFICATIONS	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 working conditions, length of deployment, security, lodging, transportation, and meals, prior to deployment

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	Same as Type 2, PLUS: The Type 1 CND Infrastructure Support Specialist serves as the supervisor for the NIMS Type 2 CND Infrastructure Support Specialist	The National Management System (NIMS) Type 2 CND Infrastructure Support Specialist works under the technical direction of a NIMS Type 1 CND Infrastructure Support Specialist to test, implement, deploy, review, and administer infrastructure hardware and software to manage computer network defenses, network services, and to monitor network activity to remediate unauthorized usage and activity	Not Specified
EDUCATION	Not Specified	Not Specified	Not Specified
TRAINING	Same as Type 2	Completion of the following: 1. IS-100: Introduction to Incident Command System, ICS-100 2. IS-200: Basic Incident Command System for Initial Response, ICS-200 3. IS-700: National Incident Management System, An Introduction 4. IS-800: National Response Framework, An Introduction 5. Information assurance and security fundamentals training at the determination of the Agency Having Jurisdiction (AHJ)	Not Specified

COMPONENT	TYPE 1	TYPE 2	NOTES
EXPERIENCE	Same as Type 2, PLUS: Applying Risk Management Framework (RMF) Security Assessment and Authorization (SAA) to specialized CND systems within the enterprise, as well as documenting and maintaining records for them or equivalent	AHJ-validated knowledge, skills, and abilities demonstrated in the following areas: 1. Data backup, types of backups, and recovery concepts and tools 2. Host and network access controls 3. Intrusion Detection System (IDS) tools and applications 4. Incident response and handling methodologies 5. Information assurance (IA) principles and organizational requirements that are relevant to confidentiality, integrity, availability, authentication, and non-repudiation 6. Network protocols 7. Traffic flows across the network 8. Packet-level analysis 9. System and application security threats and vulnerabilities 10. Network firewalls 11. Host, network, and log-based IDS hardware and software 12. Virtual Private Network (VPN) security 13. What constitutes a network attack and the relationship to both threats and vulnerabilities 14. Web filtering technologies 15. CND policies, procedures, and regulations 16. Voice-over Internet Protocol (VoIP) 17. Processes for reporting network security related incidents 18. Capabilities and Maturity Model Integration (CMMI) at all five levels 19. Network security architecture concepts, including topology, protocols, components, and principles 20. Transmission methods and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly 21. Open Systems Interconnection (OSI) 7 layer model, Transmission Control Protocol or Internet Protocol (TCP and IP), network addressing/subletting, and Virtual Local Area Networks 22. Network topologies such as 2-tier versus 3- tier segmentation (Continued)	The knowledge, skills, and abilities align with the National Initiative for Cyber Education (NICE) National Cybersecurity Workforce Framework.

COMPONENT	TYPE 1	TYPE 2	NOTES
EXPERIENCE		(Continued) 23. Defense-in-depth concepts and controls 24. Incident handling methodologies 25. Protecting a network against malware 26. Applying host access controls 27. Applying network access controls including firewalls and screening routers 28. Tuning sensors 29. Securing network communications AHJ-validated experience demonstrated in the following areas: 1. Administering CND test bed(s): testing and evaluating new CND applications; rules and signatures; access controls; and configurations of CND service provider managed platforms or equivalent 2. Managing and administering the updating of rules and signatures for specialized CND applications or equivalent 3. Creating, editing, and managing changes to network access control lists on specialized CND systems or equivalent 4. Identifying potential conflicts with implementation of any CND tools within the CND service provider area of responsibility or equivalent 5. Performing system administration on specialized CND applications and systems or VPN devices, to include installation, configuration, maintenance, and backup and restoration or equivalent 6. Assisting in identifying, prioritizing, and coordinating the protection of critical CND infrastructure and key resources 7. Creating Ethernet network cables 8. Tracing network connections 9. Terminating fiber optic cables	
PHYSICAL/MEDICAL FITNESS	Same as Type 2	Light	The NIMS Guideline for the National Qualification System (NQS) defines Physical/Medical Fitness levels for NIMS positions.
CURRENCY	Same as Type 2	1. Functions in this position during an operational incident, planned event, exercise, drill, or simulation at least once every year 2. Background checks as applicable law permits and requires 3. Active security clearance	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.

COMPONENT	TYPE 1	TYPE 2	NOTES
PROFESSIONAL AND TECHNICAL LICENSES AND CERTIFICATIONS	Same as Type 2	1. Technical qualifications equivalent to Department of Defense Directive (DoDD) 8570 Level 3 (Technical) and 8570 CND Analyst certification 2. Computer Network Administration Certification (CNAC) 3. Intrusion Analyst Certification (IAC) 4. Global Information Assurance Certification (GAIC)	Not Specified

NOTES

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

REFERENCES

1. FEMA, NIMS 508: Cyber Incident Response Team
2. FEMA, National Incident Management System (NIMS), October 2017
3. FEMA, NIMS Guideline for NQS, November 2017
4. FEMA, National Response Framework, June 2016
5. National Initiative for Cybersecurity Education, National Cybersecurity Workforce Framework, v.2, May 2014
6. Department of Defense Directive (DoDD), 8570 and Global Assurance Information Certification (GAIC), January 2014