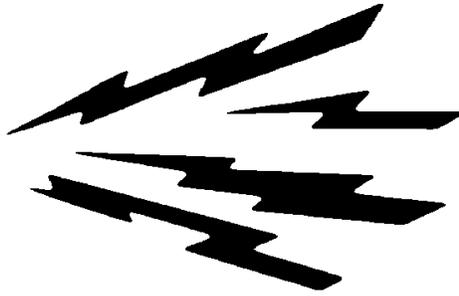


CHAPTER 67



INFORMATION SYSTEMS TECHNICIAN (IT)

NAVPERS 18068-67H

CH-76

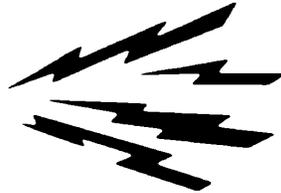
TABLE OF CONTENTS
INFORMATION SYSTEMS TECHNICIAN (IT)

SCOPE OF RATING	IT-5
GENERAL INFORMATION	IT-6
TECHNICAL SUPPORT SPECIALIST	IT-7
COMMUNICATIONS SECURITY	IT-7
COMMUNICATIONS SYSTEM OPERATIONS	IT-8
CYBERSPACE OPERATIONS	IT-8
MESSAGE SYSTEM OPERATIONS	IT-8
NETWORK ADMINISTRATION	IT-9
NETWORK MANAGEMENT	IT-10
NETWORK SYSTEM OPERATIONS	IT-10
SYSTEM ADMINISTRATOR	IT-11
COMMUNICATIONS SECURITY	IT-11
COMMUNICATIONS SYSTEM OPERATIONS	IT-12
CYBERSPACE OPERATIONS	IT-12
MESSAGE SYSTEM OPERATIONS	IT-13
NETWORK ADMINISTRATION	IT-14
NETWORK MANAGEMENT	IT-15
NETWORK SYSTEM OPERATIONS	IT-16
SYSTEMS SECURITY ANALYST	IT-17
COMMUNICATIONS SECURITY	IT-17
COMMUNICATIONS SYSTEM OPERATIONS	IT-17
CYBERSPACE OPERATIONS	IT-17
MESSAGE SYSTEM OPERATIONS	IT-18
NETWORK ADMINISTRATION	IT-19
NETWORK MANAGEMENT	IT-19
NETWORK SYSTEM OPERATIONS	IT-19
INFORMATION SYSTEMS SECURITY MANAGER	IT-20
COMMUNICATIONS SECURITY	IT-20
COMMUNICATIONS SYSTEM OPERATIONS	IT-20
CYBERSPACE OPERATIONS	IT-21

MESSAGE SYSTEM OPERATIONS	IT-22
NETWORK ADMINISTRATION	IT-22
NETWORK MANAGEMENT	IT-23
NETWORK SYSTEM OPERATIONS	IT-24
COMMUNICATION SECURITY MANAGER	IT-25
COMMUNICATIONS SECURITY	IT-25
COMMUNICATIONS SYSTEM OPERATIONS	IT-27
CYBERSPACE OPERATIONS	IT-27
MESSAGE SYSTEM OPERATIONS	IT-27
NETWORK ADMINISTRATION	IT-27
NETWORK MANAGEMENT	IT-28
NETWORK SYSTEM OPERATIONS	IT-28
CYBER DEFENSE INFRASTRUCTURE SUPPORT SPECIALIST	IT-29
COMMUNICATIONS SECURITY	IT-29
COMMUNICATIONS SYSTEM OPERATIONS	IT-29
CYBERSPACE OPERATIONS	IT-30
MESSAGE SYSTEM OPERATIONS	IT-31
NETWORK ADMINISTRATION	IT-31
NETWORK MANAGEMENT	IT-32
NETWORK SYSTEM OPERATIONS	IT-33
CYBER DEFENSE INCIDENT RESPONDER	IT-34
COMMUNICATIONS SECURITY	IT-34
COMMUNICATIONS SYSTEM OPERATIONS	IT-34
CYBERSPACE OPERATIONS	IT-35
MESSAGE SYSTEM OPERATIONS	IT-36
NETWORK ADMINISTRATION	IT-36
NETWORK MANAGEMENT	IT-37
NETWORK SYSTEM OPERATIONS	IT-38
VULNERABILITY ASSESSMENT ANALYST	IT-39
COMMUNICATIONS SECURITY	IT-39
COMMUNICATIONS SYSTEM OPERATIONS	IT-39

CYBERSPACE OPERATIONS	IT-39
MESSAGE SYSTEM OPERATIONS	IT-41
NETWORK ADMINISTRATION	IT-41
NETWORK MANAGEMENT	IT-41
NETWORK SYSTEM OPERATIONS	IT-41
RADIO FREQUENCY OPERATOR	IT-43
COMMUNICATIONS SECURITY	IT-43
COMMUNICATIONS SYSTEM OPERATIONS	IT-44
CYBERSPACE OPERATIONS	IT-46
MESSAGE SYSTEM OPERATIONS	IT-46
NETWORK ADMINISTRATION	IT-47
NETWORK MANAGEMENT	IT-48
NETWORK SYSTEM OPERATIONS	IT-48

NAVY ENLISTED OCCUPATIONAL STANDARDS
FOR
INFORMATION SYSTEMS TECHNICIAN (IT)



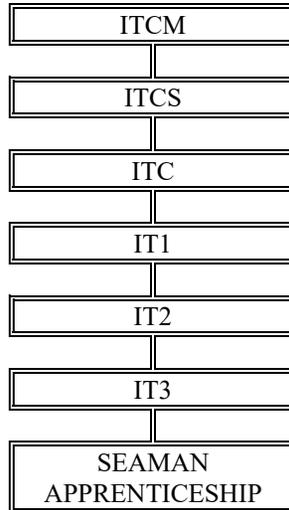
SCOPE OF RATING

Information Systems Technicians (IT) perform core and specialty functions of communications operations, message processing, network administration, and cybersecurity; secure, defend and preserve data, networks, net-centric capabilities, and other designated systems; implement security controls and defensive counter-measures; establish, monitor, and maintain Radio Frequency (RF) communications systems; perform spectrum management to support Joint, Fleet, and tactical communications; handle, store, and retrieve incoming and outgoing messages; build, configure, deploy, operate, and maintain information technology, networks and capabilities; perform network system administration, maintenance and training; manage, plan and coordinate unit-level Information Systems Security (ISS) and integration across platforms, fleets, and services; and ensure the proper security, handling, accounting, reporting, and control of Communications Security (COMSEC) materials, systems, and equipment.

These Occupational Standards are to be incorporated in Volume I, Part B, of the Manual of Navy Enlisted Manpower and Personnel Classifications and Occupational Standards (NAVPERS 18068F) as Chapter 67.

GENERAL INFORMATION

CAREER PATTERN



Normal path of advancement to Chief Warrant Officer and Limited Duty Officer categories can be found in OPNAVINST 1420.1.

For rating entry requirements, refer to MILPERSMAN 1306-618.

SAFETY

The observance of Operational Risk Management (ORM) and proper safety precautions in all areas is an integral part of each billet and the responsibility of every Sailor; therefore, it is a universal requirement for all ratings.

Job Title

Technical Support Specialist

Job Code

002776

Job Family

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

IT TECH SPECIALIST

Short Title (14 Characters)

IT TECH SPEC

Pay Plan

Enlisted

Career Field

IT

Other Relationships and Rules

NEC 745A and other NECs as assigned

Job Description

Technical Support Specialists provide end users tiered-level customer support by coordinating software, hardware, and network. May install, configure, troubleshoot, and provide maintenance and training.

DoD Relationship

Group Title

ADP Computers, General

DoD Code

115000

O*NET Relationship

Occupation Title

Computer User Support Specialists

SOC Code

15-1151.00

Job Family

Computer and Mathematical

Skills

Operation and Control

Technology Design

Critical Thinking

Complex Problem Solving

Management of Material Resources

Monitoring

Systems Analysis

Troubleshooting

Repairing

Writing

Abilities

Deductive Reasoning

Information Ordering

Control Precision

Problem Sensitivity

Inductive Reasoning

Written Comprehension

Written Expression

Flexibility of Closure

Reaction Time

Category Flexibility

COMMUNICATIONS SECURITY

Paygrade

Task Type

Task Statements

E5

NON-CORE

Administer client platform securities

E4

CORE

Conduct Emergency Action Plans (EAP)

E4

CORE

Destroy Communication Security (COMSEC) material

E4

NON-CORE

Destroy Key Management Infrastructure (KMI) products

E4

CORE

Handle Communications Security (COMSEC) material

E6

CORE

Implement Emergency Action Plans (EAP)

E4

CORE

Inspect security containers

E4

CORE

Inventory Communications Security (COMSEC) materials

E4

CORE

Load Communications Security (COMSEC) equipment

E4

CORE

Maintain Crypto Ignition Keys (CIK)

E4

CORE

Maintain cryptographic equipment

E4

CORE

Maintain physical security of Sensitive Compartmented Information (SCI) Information Systems (IS)

E4

CORE

Receive Communications Security (COMSEC) material

E4

CORE

Report Communications Security (COMSEC) discrepancies

E4

CORE

Set up cryptographic equipment

E4

CORE

Set up cryptographic networks

E4

CORE

Validate Communications Security (COMSEC) material

E4

CORE

Verify cryptographic equipment settings

COMMUNICATIONS SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Configure router and switching devices
E5	CORE	Coordinate restoral with off site technicians
E6	CORE	Develop Combat System Training Team (CSTT) scenarios
E5	NON-CORE	Integrate flight and squadron media
E4	CORE	Load image software
E4	CORE	Load magnetic tape
E4	CORE	Maintain magnetic tape drives
E4	CORE	Monitor routing and switching devices
E4	CORE	Restore computer Information Systems (IS)
E5	CORE	Restore loss of Facilities Control (FACCON)

CYBERSPACE OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Determine patterns of non-compliance (e.g., risk levels, Information Assurance (IA) program effectiveness, etc.)
E4	CORE	Identify Information Systems Security (ISS) violations and vulnerabilities
E4	CORE	Identify security issues (i.e., protection, aggregation, inter-connectivity)
E5	NON-CORE	Implement Information Assurance Vulnerability Alerts (IAVA)
E5	NON-CORE	Implement Information Assurance Vulnerability Bulletins (IAVB)
E5	CORE	Implement security actions
E5	CORE	Maintain Information Systems (IS) logs
E5	NON-CORE	Perform real-time cyber defense incident handling tasks (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation, etc.)
E4	NON-CORE	Provide technical support to resolve cyber incidents
E4	NON-CORE	Remove system viruses
E7	NON-CORE	Report Information Systems Security (ISS) incidents
E4	CORE	Update computer Information Systems (IS) antivirus definitions
E6	NON-CORE	Validate migration/installation computer software

MESSAGE SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Establish Command, Control, Communications, Computers, Combat Systems and Intelligence (C5I) system interconnectivity
E4	NON-CORE	Install certificates (e.g., security, system, etc.)
E4	CORE	Maintain local media and technical libraries
E5	CORE	Manage messaging systems
E4	CORE	Monitor message queues
E4	CORE	Monitor message systems
E7	NON-CORE	Validate unit and command certificates

NETWORK ADMINISTRATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	NON-CORE	Administer Information Systems (IS) accounts
E5	CORE	Analyze logs
E4	CORE	Back up Information Systems (IS)
E4	CORE	Configure computer application software
E4	NON-CORE	Configure network hardware
E5	NON-CORE	Configure network services
E4	CORE	Configure peripherals
E5	NON-CORE	Configure virus scanners
E4	NON-CORE	Configure workstation network connectivity
E4	CORE	Configure workstation Operating System (OS) software
E5	CORE	Develop Information Systems (IS) Standard Operating Procedures (SOP)
E5	CORE	Document Information Systems (IS) errors
E4	CORE	Document network outages
E5	CORE	Document off-site technical support actions
E5	CORE	Document server outages
E6	CORE	Implement remediation plans for identified vulnerabilities
E4	NON-CORE	Implement River City conditions on Information Systems (IS)
E4	NON-CORE	Install network components
E4	CORE	Install network peripherals
E4	NON-CORE	Install network software
E4	CORE	Install Operating Systems (OS)
E4	CORE	Install peripherals
E4	CORE	Isolate infected systems
E6	CORE	Maintain network documentation
E4	CORE	Maintain network printers
E5	NON-CORE	Manage file and folder access
E5	NON-CORE	Manage network monitoring software
E4	CORE	Monitor network equipment status
E4	CORE	Patch Information Systems (IS)
E4	CORE	Perform disk administration
E4	CORE	Perform file system maintenance
E4	CORE	Perform File Transfer Protocol (FTP) functions
E4	CORE	Perform start up/shut down procedures
E5	NON-CORE	Perform trend analysis (hardware, software, or network)
E5	CORE	Prepare network status reports
E4	CORE	Respond to customer trouble calls
E4	CORE	Review logs
E4	CORE	Scan for viruses

NETWORK ADMINISTRATION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Test computer Information Systems (IS)
E4	CORE	Troubleshoot client Operating Systems (OS)
E4	CORE	Troubleshoot file and folder access problems
E4	CORE	Troubleshoot network hardware
E4	CORE	Troubleshoot peripherals
E5	CORE	Troubleshoot storage devices
E4	CORE	Troubleshoot workstation application software
E4	CORE	Troubleshoot workstation network connectivity
E5	CORE	Verify network system operations

NETWORK MANAGEMENT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Conduct computer software migration
E7	CORE	Implement Information Systems (IS) equipment and media disposition requirements (e.g., destruction, disposal, transfer, etc.)
E5	CORE	Restore from backups
E4	CORE	Troubleshoot network cabling
E5	NON-CORE	Troubleshoot Wide Area Network (WAN)
E4	CORE	Verify backups

NETWORK SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Administer network system databases
E6	NON-CORE	Coordinate Information Systems (IS) backup
E5	NON-CORE	Identify Information Systems (IS) anomalies
E7	CORE	Implement network operating procedures
E4	CORE	Inspect Information Systems (IS) (e.g., network components, system hardware, etc.)
E4	CORE	Install Information Systems (IS) components (e.g., system hardware, storage devices, etc.)
E4	CORE	Inventory Information Systems (IS) assets
E7	CORE	Maintain Information Systems (IS) (e.g., Program of Record (POR), authorized, etc.)
E5	CORE	Perform data transfers
E5	CORE	Process customer trouble calls
E5	NON-CORE	Troubleshoot networks (e.g., Integrated Shipboard Network Systems (ISNS), Consolidated Afloat Networks and Enterprise Services (CANES), virtual, etc.)
E4	NON-CORE	Troubleshoot virtual environments

Job Title**System Administrator****Job Code****002777****Job Family**

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

SYSTEM ADMINISTRATOR

Short Title (14 Characters)

SYS ADMIN

Pay Plan

Enlisted

Career Field

IT

Other Relationships and Rules

NEC 746A and other NECs as assigned

Job Description

System Administrators install, configure, troubleshoot, and maintain server and systems configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Administers server-based systems, security devices, distributed applications, network storage, messaging, and performs systems monitoring. Consults on network, application, and customer service issues to support computer systems' security and sustainability.

DoD Relationship**Group Title**

ADP Computers, General

DoD Code

115000

O*NET Relationship**Occupation Title**

Network and Computer Systems Administrators

SOC Code

15-1142.00

Job Family

Computer and Mathematical

Skills*Operation and Control**Technology Design**Critical Thinking**Management of Material Resources**Complex Problem Solving**Systems Analysis**Troubleshooting**Monitoring**Repairing**Writing***Abilities***Deductive Reasoning**Information Ordering**Control Precision**Problem Sensitivity**Inductive Reasoning**Written Comprehension**Written Expression**Flexibility of Closure**Oral Expression**Reaction Time***COMMUNICATIONS SECURITY****Paygrade**

E5

Task Type

NON-CORE

Task Statements

Administer client platform securities

E4

CORE

Conduct Emergency Action Plans (EAP)

E4

CORE

Destroy Communication Security (COMSEC) material

E4

NON-CORE

Destroy Key Management Infrastructure (KMI) products

E6

CORE

Develop Emergency Action Plans (EAP)

E4

CORE

Handle Communications Security (COMSEC) material

E4

CORE

Identify Communications Security (COMSEC) discrepancies

E6

CORE

Implement Communications Security (COMSEC) changes

E6

CORE

Implement Emergency Action Plans (EAP)

E4

CORE

Inspect security containers

E4

CORE

Inventory Communications Security (COMSEC) materials

E4

CORE

Load Communications Security (COMSEC) equipment

E4

CORE

Maintain Crypto Ignition Keys (CIK)

E4

CORE

Maintain cryptographic equipment

E4

CORE

Maintain physical security of Sensitive Compartmented Information (SCI) Information Systems (IS)

E5

CORE

Prepare local element Communication Security (COMSEC) reports

E4

CORE

Receive Communications Security (COMSEC) material

COMMUNICATIONS SECURITY (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Report Communications Security (COMSEC) discrepancies
E4	CORE	Set up cryptographic equipment
E4	CORE	Set up cryptographic networks
E6	NON-CORE	Transfer custody of Communications Security (COMSEC) material
E4	CORE	Validate Communications Security (COMSEC) material
E4	CORE	Verify cryptographic equipment settings

COMMUNICATIONS SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Configure router and switching devices
E5	CORE	Coordinate restoral with off site technicians
E5	NON-CORE	Determine system configuration requirements
E6	CORE	Develop Combat System Training Team (CSTT) scenarios
E4	CORE	Forecast service demands
E4	NON-CORE	Initialize magnetic tapes drives
E5	NON-CORE	Integrate flight and squadron media
E5	NON-CORE	Integrate Intelligence, Surveillance, and Reconnaissance (ISR) services (e.g., Global Broadcasting Systems (GBS), Communications Data Link System (CDLS), etc.)
E5	CORE	Investigate loss of Facilities Control (FACCON)
E4	CORE	Load image software
E4	CORE	Load magnetic tape
E4	CORE	Maintain magnetic tape drives
E4	CORE	Monitor routing and switching devices
E4	CORE	Perform End of Mission Sanitizations (EOMS)
E4	NON-CORE	Perform Information Systems (IS) backups
E5	NON-CORE	Perform Internet Protocol (IP) shift
E4	CORE	Restore computer Information Systems (IS)
E5	CORE	Restore loss of Facilities Control (FACCON)
E4	CORE	Set Emission Control (EMCON) conditions
E5	NON-CORE	Troubleshoot router and switching devices

CYBERSPACE OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	CORE	Complete network security assessment checklists
E5	NON-CORE	Configure network firewalls
E7	CORE	Determine patterns of non-compliance (e.g., risk levels, Information Assurance (IA) program effectiveness, etc.)
E7	NON-CORE	Ensure procedures and guidelines comply with cybersecurity policies
E6	NON-CORE	Evaluate Information Systems Security (ISS)
E7	CORE	Forecast service demands

CYBERSPACE OPERATIONS (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Identify Information Systems Security (ISS) violations and vulnerabilities
E4	CORE	Identify security issues (i.e., protection, aggregation, inter-connectivity)
E5	NON-CORE	Implement Information Assurance Vulnerability Alerts (IAVA)
E5	NON-CORE	Implement Information Assurance Vulnerability Bulletins (IAVB)
E6	NON-CORE	Implement Information Systems Security (ISS) policies
E6	CORE	Implement network security applications
E5	NON-CORE	Implement policies and procedures to ensure protection of critical infrastructure
E5	CORE	Implement security actions
E5	CORE	Maintain Information Systems (IS) logs
E5	NON-CORE	Perform cybersecurity assessments
E5	NON-CORE	Perform real-time cyber defense incident handling tasks (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation, etc.)
E4	NON-CORE	Provide technical support to resolve cyber incidents
E7	CORE	Recommend new information technology security requirements
E4	NON-CORE	Remove system viruses
E6	NON-CORE	Report Information Security (INFOSEC) compliance
E7	NON-CORE	Report Information Systems Security (ISS) incidents
E7	CORE	Review Information Systems Security (ISS) requirements
E6	NON-CORE	Track audit findings for mitigation actions
E4	CORE	Update computer Information Systems (IS) antivirus definitions
E6	NON-CORE	Validate migration/installation computer software
E6	NON-CORE	Validate network security improvement actions

MESSAGE SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Configure message processing systems
E4	CORE	Download naval messages via automated systems
E5	CORE	Establish Command, Control, Communications, Computers, Combat Systems and Intelligence (C5I) system interconnectivity
E5	CORE	Implement non-repudiation controls
E4	NON-CORE	Install certificates (e.g., security, system, etc.)
E4	CORE	Maintain local media and technical libraries
E5	CORE	Manage messaging systems
E4	CORE	Monitor message queues
E4	CORE	Monitor message systems
E4	CORE	Perform minimize condition procedures
E7	NON-CORE	Validate unit and command certificates

NETWORK ADMINISTRATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	NON-CORE	Administer Information Systems (IS) accounts
E5	CORE	Analyze logs
E4	CORE	Back up Information Systems (IS)
E4	CORE	Configure computer application software
E5	CORE	Configure logs
E4	NON-CORE	Configure network hardware
E5	NON-CORE	Configure network services
E4	CORE	Configure peripherals
E5	NON-CORE	Configure router Access Control Lists (ACL)
E5	NON-CORE	Configure server Operating System (OS) software
E5	NON-CORE	Configure virus scanners
E4	NON-CORE	Configure workstation network connectivity
E4	CORE	Configure workstation Operating System (OS) software
E4	NON-CORE	Construct networks
E5	CORE	Develop Information Systems (IS) Standard Operating Procedures (SOP)
E5	CORE	Document Information Systems (IS) errors
E4	CORE	Document network outages
E5	CORE	Document off-site technical support actions
E5	CORE	Document server outages
E6	CORE	Implement remediation plans for identified vulnerabilities
E4	NON-CORE	Implement River City conditions on Information Systems (IS)
E5	NON-CORE	Initialize network servers
E4	NON-CORE	Install network components
E4	CORE	Install network peripherals
E4	NON-CORE	Install network software
E4	CORE	Install Operating Systems (OS)
E4	CORE	Install peripherals
E4	CORE	Isolate infected systems
E5	NON-CORE	Maintain Information Systems (IS) servers
E6	CORE	Maintain network documentation
E4	CORE	Maintain network printers
E7	CORE	Manage audit data
E5	NON-CORE	Manage file and folder access
E5	NON-CORE	Manage Information Systems (IS) queues
E5	NON-CORE	Manage Information Systems (IS) servers
E5	NON-CORE	Manage network monitoring software
E6	NON-CORE	Manage network system configurations
E6	NON-CORE	Manage network system updates

NETWORK ADMINISTRATION (CONT'D)

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Monitor network equipment status
E4	CORE	Patch Information Systems (IS)
E4	CORE	Perform disk administration
E4	CORE	Perform file system maintenance
E4	CORE	Perform File Transfer Protocol (FTP) functions
E4	CORE	Perform start up/shut down procedures
E5	NON-CORE	Perform trend analysis (hardware, software, or network)
E7	NON-CORE	Plan network restorations
E5	CORE	Prepare network status reports
E4	CORE	Respond to customer trouble calls
E4	CORE	Review logs
E4	CORE	Scan for viruses
E4	CORE	Test computer Information Systems (IS)
E4	CORE	Troubleshoot client Operating Systems (OS)
E4	CORE	Troubleshoot file and folder access problems
E4	CORE	Troubleshoot network hardware
E4	CORE	Troubleshoot peripherals
E5	NON-CORE	Troubleshoot server Operating Systems (OS)
E5	CORE	Troubleshoot storage devices
E4	CORE	Troubleshoot workstation application software
E4	CORE	Troubleshoot workstation network connectivity
E5	NON-CORE	Update network policies
E5	CORE	Verify network system operations

NETWORK MANAGEMENT

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Conduct computer software migration
E5	NON-CORE	Configure domain system policies
E7	NON-CORE	Determine network migration and installation potential problems
E7	CORE	Develop disaster recovery contingency plans
E7	NON-CORE	Develop system life cycle plans
E6	NON-CORE	Draft network topologies
E7	NON-CORE	Estimate network migration or installation costs
E6	NON-CORE	Implement domain policies
E7	CORE	Implement Information Systems (IS) equipment and media disposition requirements (e.g., destruction, disposal, transfer, etc.)
E6	NON-CORE	Implement network policies
E5	NON-CORE	Maintain network topologies
E7	NON-CORE	Manage Local Area Network (LAN) architecture

NETWORK MANAGEMENT (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	NON-CORE	Manage network system databases
E7	NON-CORE	Manage networking solutions
E7	NON-CORE	Plan network upgrades
E7	NON-CORE	Provide incident details to external organizations (e.g., law enforcement personnel)
E5	CORE	Restore from backups
E4	CORE	Troubleshoot network cabling
E5	NON-CORE	Troubleshoot Wide Area Network (WAN)
E7	CORE	Validate baseline security safeguard installation
E4	CORE	Verify backups

NETWORK SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Administer network system databases
E5	NON-CORE	Configure virtual environments
E4	CORE	Configure workstation core components
E6	NON-CORE	Coordinate Information Systems (IS) backup
E5	NON-CORE	Develop web pages
E5	NON-CORE	Identify Information Systems (IS) anomalies
E7	CORE	Implement network operating procedures
E4	CORE	Inspect Information Systems (IS) (e.g., network components, system hardware, etc.)
E4	CORE	Install Information Systems (IS) components (e.g., system hardware, storage devices, etc.)
E5	NON-CORE	Install servers
E4	CORE	Inventory Information System (IS) assets
E5	NON-CORE	Maintain Cross-Domain solutions
E7	CORE	Maintain Information Systems (IS) (e.g., Program of Record (POR), authorized, etc.)
E5	CORE	Maintain network system databases
E5	CORE	Maintain software application scripts
E5	NON-CORE	Maintain websites
E5	CORE	Perform data transfers
E5	CORE	Process customer trouble calls
E5	NON-CORE	Troubleshoot networks (e.g., Integrated Shipboard Network Systems (ISNS), Consolidated Afloat Networks and Enterprise Services (CANES), virtual, etc.)
E4	NON-CORE	Troubleshoot virtual environments
E6	NON-CORE	Write software application scripts

Job Title

Systems Security Analyst

Job Code

002778

Job Family

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

SYSTEMS SECURITY ANALYST

Short Title (14 Characters)

SYS SEC ANAL

Pay Plan

Enlisted

Career Field

IT

Other Relationships and Rules

NEC 742A and other NECs as assigned

Job Description

Systems Security Analysts conduct the integration/testing, operation, and maintenance of systems security.

DoD Relationship

O*NET Relationship

Group Title

ADP Computers, General

DoD Code

115000

Occupation Title

Information Security Analysts

SOC Code

15-1122.00

Job Family

Computer and Mathematical

Skills

Operation and Control
Critical Thinking
Complex Problem Solving
Management of Material Resources
Technology Design
Monitoring
Writing
Operations Analysis
Systems Evaluation
Quality Control Analysis

Abilities

Deductive Reasoning
Information Ordering
Inductive Reasoning
Control Precision
Problem Sensitivity
Written Comprehension
Written Expression
Perceptual Speed
Flexibility of Closure
Oral Expression

COMMUNICATIONS SECURITY

Paygrade

Task Type

Task Statements

E5	NON-CORE	Administer client platform securities
E4	CORE	Conduct Emergency Action Plans (EAP)
E4	CORE	Destroy Communication Security (COMSEC) material
E4	NON-CORE	Destroy Key Management Infrastructure (KMI) products
E6	NON-CORE	Develop system security certification and accreditation documents
E4	CORE	Handle Communications Security (COMSEC) material
E4	CORE	Inspect security containers
E4	CORE	Maintain physical security of Sensitive Compartmented Information (SCI) Information Systems (IS)
E4	CORE	Report Communications Security (COMSEC) discrepancies

COMMUNICATIONS SYSTEM OPERATIONS

Paygrade

Task Type

Task Statements

E5	CORE	Coordinate restoral with off-site technicians
E6	CORE	Develop Combat System Training Team (CSTT) scenarios

CYBERSPACE OPERATIONS

Paygrade

Task Type

Task Statements

E5	NON-CORE	Analyze Information Systems Security (ISS) posture trends
E5	NON-CORE	Analyze malicious activity
E5	NON-CORE	Analyze metadata in network traffic
E6	CORE	Complete network security assessment checklists

CYBERSPACE OPERATIONS (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Configure network firewalls
E7	CORE	Determine patterns of non-compliance (e.g., risk levels, Information Assurance (IA) program effectiveness, etc.)
E6	NON-CORE	Evaluate Information Systems Security (ISS)
E7	NON-CORE	Evaluate Information Systems Security (ISS) incidents
E7	CORE	Evaluate security improvement actions
E5	NON-CORE	Identify applications and Operating Systems (OS) of a network device based on network traffic
E4	CORE	Identify Information Systems Security (ISS) violations and vulnerabilities
E5	NON-CORE	Identify network mapping and Operating System (OS) fingerprinting activities
E4	CORE	Identify security issues (i.e., protection, aggregation, inter-connectivity)
E6	NON-CORE	Implement alternative Information Security (INFOSEC) strategies
E5	NON-CORE	Implement Information Assurance Vulnerability Alerts (IAVA)
E5	NON-CORE	Implement Information Assurance Vulnerability Bulletins (IAVB)
E6	NON-CORE	Implement Information Systems Security (ISS) policies
E6	CORE	Implement network security applications
E5	NON-CORE	Implement policies and procedures to ensure protection of critical infrastructure
E5	CORE	Implement security actions
E5	NON-CORE	Isolate malicious code
E5	NON-CORE	Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware)
E5	CORE	Maintain Information Systems (IS) logs
E5	NON-CORE	Perform cybersecurity assessments
E5	NON-CORE	Perform real-time cyber defense incident handling tasks (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation, etc.)
E4	NON-CORE	Provide technical support to resolve cyber incidents
E5	NON-CORE	Reconstruct a malicious attack or activity based off network traffic
E4	NON-CORE	Remove system viruses
E7	NON-CORE	Report Information Systems Security (ISS) incidents
E5	NON-CORE	Report organizational security posture trends
E7	CORE	Review Information Systems Security (ISS) requirements
E6	NON-CORE	Track audit findings for mitigation actions
E4	CORE	Update computer Information Systems (IS) antivirus definitions
E5	NON-CORE	Validate Intrusion Detection System (IDS) alerts
E6	NON-CORE	Validate network security improvement actions

MESSAGE SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Maintain local media and technical libraries

NETWORK ADMINISTRATION

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Analyze logs
E5	CORE	Document Information Systems (IS) errors
E5	CORE	Document off-site technical support actions
E6	CORE	Implement remediation plans for identified vulnerabilities
E4	NON-CORE	Implement River City conditions on Information Systems (IS)
E4	CORE	Isolate infected systems
E6	CORE	Maintain network documentation
E7	CORE	Manage audit data
E5	NON-CORE	Manage network monitoring software
E4	CORE	Monitor network equipment status
E4	CORE	Perform start up/shut down procedures
E5	NON-CORE	Perform trend analysis (hardware, software, or network)
E5	CORE	Prepare network status reports
E4	CORE	Review logs
E4	CORE	Scan for viruses
E4	CORE	Test computer Information Systems (IS)
E4	CORE	Troubleshoot client Operating Systems (OS)

NETWORK MANAGEMENT

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	NON-CORE	Provide incident details to external organizations (e.g., law enforcement personnel)
E5	NON-CORE	Report Information Systems (IS) security posture trends
E5	NON-CORE	Troubleshoot Wide Area Network (WAN)
E7	CORE	Validate baseline security safeguard installation

NETWORK SYSTEM OPERATIONS

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Administer network system databases
E5	NON-CORE	Identify Information Systems (IS) anomalies
E4	CORE	Inventory Information System (IS) assets
E7	CORE	Maintain Information Systems (IS) (e.g., Program of Record (POR), authorized, etc.)
E5	CORE	Maintain software application scripts

Job Title

Information Systems Security Manager

Job Code

002779

Job Family

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

INFO SYSTEMS SECURITY MANAGER

Short Title (14 Characters)

ISSM

Pay Plan

Enlisted

Career Field

IT

Other Relationships and Rules

NEC 741A and other NECs as assigned

Job Description

Information Systems Security Managers oversee the cybersecurity program of an information system or network; including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.

DoD Relationship

Group Title

ADP Computers, General

DoD Code

115000

O*NET Relationship

Occupation Title

Network and Computer Systems Administrators

SOC Code

15-1142.00

Job Family

Computer and Mathematical

Skills

Operation and Control
Critical Thinking
Management of Material Resources
Complex Problem Solving
Writing
Technology Design
Coordination
Quality Control Analysis
Monitoring
Operations Analysis

Abilities

Deductive Reasoning
Information Ordering
Inductive Reasoning
Written Expression
Problem Sensitivity
Written Comprehension
Control Precision
Oral Expression
Flexibility of Closure
Perceptual Speed

COMMUNICATIONS SECURITY

Paygrade

Task Type

Task Statements

E5	NON-CORE	Administer client platform securities
E5	NON-CORE	Administer token securities
E4	CORE	Conduct Emergency Action Plans (EAP)
E4	CORE	Destroy Communication Security (COMSEC) material
E4	NON-CORE	Destroy Key Management Infrastructure (KMI) products
E6	CORE	Develop Emergency Action Plans (EAP)
E6	NON-CORE	Develop Information Systems Security (ISS) plans
E6	NON-CORE	Develop network security instructions
E6	NON-CORE	Develop system security certification and accreditation documents
E4	CORE	Inspect security containers
E4	CORE	Maintain physical security of Sensitive Compartmented Information (SCI) Information Systems (IS)
E4	CORE	Report Communications Security (COMSEC) discrepancies

COMMUNICATIONS SYSTEM OPERATIONS

Paygrade

Task Type

Task Statements

E5	CORE	Coordinate restoral with off-site technicians
E5	NON-CORE	Determine system configuration requirements
E6	CORE	Develop Combat System Training Team (CSTT) scenarios

COMMUNICATIONS SYSTEM OPERATIONS (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	NON-CORE	Verify system certifications

CYBERSPACE OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Advise leadership of changes affecting the organization's cybersecurity posture
E5	NON-CORE	Analyze Information Systems Security (ISS) posture trends
E5	NON-CORE	Analyze organizational security posture trends
E6	NON-CORE	Assess the impact of implementing and sustaining a dedicated cyber defense infrastructure
E6	CORE	Complete network security assessment checklists
E7	NON-CORE	Coordinate the protection of critical cyber defense infrastructure and key resources
E7	CORE	Determine patterns of non-compliance (e.g., risk levels, Information Assurance (IA) program effectiveness, etc.)
E6	NON-CORE	Determine potential conflicts with implementation of any cyber defense tools (e.g., tools and signature, testing and optimization)
E7	NON-CORE	Develop critical infrastructure protection policies and procedures
E7	NON-CORE	Develop domain policies
E7	NON-CORE	Develop Information Systems Security (ISS) policies
E5	NON-CORE	Disseminate cyber defense techniques and guidance (e.g., Time Compliance Network Orders [TCNO], concept of operations, net analyst reports, etc.) for the organization
E5	CORE	Disseminate technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters
E7	CORE	Draft Continuity of Operations Program (COOP)
E7	NON-CORE	Ensure procedures and guidelines comply with cybersecurity policies
E6	NON-CORE	Evaluate Information Systems Security (ISS)
E7	CORE	Evaluate security improvement actions
E7	NON-CORE	Identify critical cyber defense infrastructure and key resources
E4	CORE	Identify Information Systems Security (ISS) violations and vulnerabilities
E7	NON-CORE	Identify Information Technology (IT) security program implications of new technologies or technology upgrades
E4	CORE	Identify security issues (i.e., protection, aggregation, inter-connectivity)
E6	NON-CORE	Implement alternative Information Security (INFOSEC) strategies
E6	NON-CORE	Implement Information Systems Security (ISS) policies
E6	CORE	Implement network security applications
E5	NON-CORE	Implement policies and procedures to ensure protection of critical infrastructure
E5	CORE	Implement security actions
E5	NON-CORE	Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware, etc.)
E7	NON-CORE	Maintain Information Systems Security (ISS) certification and accreditation documentation

CYBERSPACE OPERATIONS (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Manage cybersecurity workforce programs
E7	NON-CORE	Manage electronic spillage process
E7	NON-CORE	Manage Information Security (INFOSEC) incident reporting processes
E7	CORE	Manage Information Security (INFOSEC) training and awareness programs
E7	NON-CORE	Manage Information Systems Security (ISS) programs
E7	CORE	Manage Information Technology (IT) resources and security personnel
E7	CORE	Manage Information Technology (IT) security priorities
E7	NON-CORE	Manage intranet/Department of Defense Information Network (DODIN) security policies
E5	NON-CORE	Perform cybersecurity assessments
E5	NON-CORE	Perform real-time cyber defense incident handling tasks (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation, etc.)
E4	NON-CORE	Provide technical support to resolve cyber incidents
E7	CORE	Recommend new information technology security requirements
E5	NON-CORE	Reconstruct a malicious attack or activity based off network traffic
E6	NON-CORE	Report Information Security (INFOSEC) compliance
E7	NON-CORE	Report Information Systems Security (ISS) incidents
E5	NON-CORE	Report organizational security posture trends
E7	CORE	Review Information Systems Security (ISS) requirements
E7	CORE	Review security risk assumption
E6	NON-CORE	Track audit findings for mitigation actions
E5	NON-CORE	Validate Intrusion Detection System (IDS) alerts
E6	NON-CORE	Validate migration/installation computer software
E6	NON-CORE	Validate network security improvement actions
E7	NON-CORE	Verify acquisitions, procurements, and outsourcing efforts of Information Security (INFOSEC) requirements

MESSAGE SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Maintain local media and technical libraries

NETWORK ADMINISTRATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Analyze logs
E5	CORE	Develop Information System (IS) Standard Operating Procedures (SOP)
E5	CORE	Document Information Systems (IS) errors
E5	CORE	Document off-site technical support actions
E6	CORE	Implement remediation plans for identified vulnerabilities
E6	CORE	Maintain network documentation
E7	CORE	Manage audit data

NETWORK ADMINISTRATION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Manage Information Systems (IS) servers
E5	NON-CORE	Manage network monitoring software
E6	NON-CORE	Manage network system configurations
E6	NON-CORE	Manage network system updates
E5	NON-CORE	Perform trend analysis (hardware, software, or network)
E7	NON-CORE	Plan network restorations
E5	CORE	Prepare network status reports
E4	CORE	Review logs
E5	NON-CORE	Update network policies

NETWORK MANAGEMENT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	NON-CORE	Advise senior management (i.e., CIO) on cost/benefit analysis of Information Security (INFOSEC) programs, policies, processes, systems, and elements
E5	NON-CORE	Conduct computer software migration
E7	CORE	Coordinate cybersecurity inspections, tests, and reviews
E7	NON-CORE	Determine network migration and installation potential problems
E7	NON-CORE	Determine network migrations and installation time requirements
E7	CORE	Develop disaster recovery contingency plans
E7	NON-CORE	Develop network plans and policies
E7	CORE	Develop remediation plans for identified vulnerabilities
E7	NON-CORE	Develop system life cycle plans
E6	NON-CORE	Draft network topologies
E7	NON-CORE	Estimate network migration or installation costs
E7	NON-CORE	Evaluate cost-benefit, economic, and risk analysis in decision-making process
E6	NON-CORE	Implement domain policies
E7	CORE	Implement Information Systems (IS) equipment and media disposition requirements (e.g., destruction, disposal, transfer, etc.)
E6	NON-CORE	Implement network policies
E7	NON-CORE	Maintain Information Technology (IT) security requirements in all phases of the System Life Cycle
E5	NON-CORE	Maintain network topologies
E7	NON-CORE	Maintain Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems
E7	NON-CORE	Manage Local Area Network (LAN) architecture
E7	NON-CORE	Manage networking solutions
E7	NON-CORE	Oversee Information Security (INFOSEC) budget, staffing, and contracting
E7	NON-CORE	Provide incident details to external organizations (e.g., law enforcement personnel)
E5	NON-CORE	Report Information Systems Security (ISS) posture trends
E7	CORE	Validate baseline security safeguard installation

NETWORK SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Implement network operating procedures
E4	CORE	Inspect Information Systems (IS) (e.g., network components, system hardware, etc.)
E4	CORE	Inventory Information Systems (IS) assets
E5	NON-CORE	Maintain Cross-Domain solutions
E5	CORE	Perform data transfers

Job Title

Communication Security Manager

Job Code

002780

Job Family
Management

NOC
TBD

Short Title (30 Characters)
COMMUNICATION SECURITY

Short Title (14 Characters)
COMSEC MANAGER

Pay Plan
Enlisted

Career Field
IT

Other Relationships and Rules
NEC H04A and other NECs as assigned

Job Description

Communication Security Managers oversee the cybersecurity program of an information system or network; including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.

DoD Relationship

Group Title **DoD Code**
ADP Computers, General 115000

O*NET Relationship

Occupation Title **SOC Code** **Job Family**
Computer and Information 11-3021.00 Management
Systems Managers

Skills

- Operation and Control*
- Critical Thinking*
- Management of Material Resources*
- Technology Design*
- Systems Analysis*
- Writing*
- Complex Problem Solving*
- Monitoring*
- Installation*
- Systems Evaluation*

Abilities

- Information Ordering*
- Deductive Reasoning*
- Inductive Reasoning*
- Control Precision*
- Written Comprehension*
- Problem Sensitivity*
- Written Expression*
- Category Flexibility*
- Oral Expression*
- Flexibility of Closure*

COMMUNICATIONS SECURITY

Paygrade

Task Type

Task Statements

E6	NON-CORE	Administer access to symmetric Crypto Net Key Management Infrastructure (KMI)
E5	NON-CORE	Administer client platform securities
E6	NON-CORE	Administer client platforms Key Management Infrastructure (KMI)
E5	NON-CORE	Administer deployed cryptologic tactical systems Key Management Infrastructure (KMI)
E6	NON-CORE	Administer High Assurance Platform (HAP) securities
E6	NON-CORE	Administer High Assurance Platforms (HAP)
E6	NON-CORE	Administer Key Management Infrastructure (KMI) Key Operating Accounts (KOA)
E5	NON-CORE	Administer Key Management Infrastructure (KMI) user accounts
E5	NON-CORE	Administer token securities
E6	NON-CORE	Assign product requestors
E6	NON-CORE	Audit Key Management Infrastructure (KMI) management data
E5	NON-CORE	Back up Key Management Infrastructure (KMI) accounts
E6	CORE	Brief communications security roles, responsibilities, obligations, and liabilities
E4	CORE	Conduct Emergency Action Plans (EAP)
E6	NON-CORE	Deregister Key Management Infrastructure (KMI) devices
E4	CORE	Destroy Communication Security (COMSEC) material
E4	NON-CORE	Destroy Key Management Infrastructure (KMI) products

COMMUNICATIONS SECURITY (CONT'D)

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	CORE	Develop Emergency Action Plans (EAP)
E6	NON-CORE	Develop local Communications Security (COMSEC) handling instructions
E6	NON-CORE	Endorse Key Management Infrastructure (KMI) devices
E6	NON-CORE	Establish Key Management Infrastructure (KMI) new product requirements
E6	NON-CORE	Generate Key Management Infrastructure (KMI) cryptologic product requests
E5	NON-CORE	Generate Key Management Infrastructure (KMI) local electronic keys
E5	NON-CORE	Generate local keys
E4	CORE	Handle Communications Security (COMSEC) material
E4	CORE	Identify Communications Security (COMSEC) discrepancies
E6	CORE	Implement Communications Security (COMSEC) changes
E6	CORE	Implement Emergency Action Plans (EAP)
E6	NON-CORE	Initialize access to asymmetric cryptologic network
E5	NON-CORE	Initialize Key Management Infrastructure (KMI) devices
E4	CORE	Inspect security containers
E4	CORE	Inventory Communications Security (COMSEC) materials
E5	NON-CORE	Issue Communication Security (COMSEC) material
E5	NON-CORE	Issue Key Management Infrastructure (KMI) materials
E4	CORE	Load Communications Security (COMSEC) equipment
E4	CORE	Maintain Crypto Ignition Keys (CIK)
E4	CORE	Maintain cryptographic equipment
E5	NON-CORE	Maintain Communications Security (COMSEC) databases
E6	NON-CORE	Maintain Key Management Infrastructure (KMI) databases
E4	CORE	Maintain physical security of Sensitive Compartmented Information (SCI) Information Systems (IS)
E6	CORE	Manage Communications Security (COMSEC) training programs
E6	NON-CORE	Manage Key Management Infrastructure (KMI) Device Distribution Profiles (DDP)
E5	NON-CORE	Manage Key Management Infrastructure (KMI) network connectivity
E6	NON-CORE	Manage Key Management Infrastructure (KMI) production
E5	NON-CORE	Manage Key Management Infrastructure (KMI) system configuration
E5	NON-CORE	Manage Key Management Infrastructure (KMI) system reports
E5	NON-CORE	Manage Key Management Infrastructure (KMI) tokens
E6	CORE	Monitor Communications Security (COMSEC) platform security
E6	NON-CORE	Order Communications Security (COMSEC) products
E5	NON-CORE	Perform personalization of type 1 tokens
E5	CORE	Prepare local element Communication Security (COMSEC) reports
E4	CORE	Process Communications Security (COMSEC) changes
E4	CORE	Receive Communications Security (COMSEC) material
E6	NON-CORE	Register Communications Security (COMSEC) users

COMMUNICATIONS SECURITY (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	NON-CORE	Register Key Management Infrastructure (KMI) Key Operating Account (KOA) agents
E5	NON-CORE	Register Key Management Infrastructure (KMI) users
E6	NON-CORE	Register local Communications Security (COMSEC) elements
E6	CORE	Report Communications Security (COMSEC) compliance
E4	CORE	Report Communications Security (COMSEC) discrepancies
E5	NON-CORE	Review Key Management Infrastructure (KMI) databases
E4	CORE	Set up cryptographic equipment
E4	CORE	Set up cryptographic networks
E6	NON-CORE	Transfer custody of Communications Security (COMSEC) material
E6	NON-CORE	Troubleshoot Key Processors (KP)
E6	NON-CORE	Update Device Distribution Profiles (DDP)
E4	CORE	Validate Communications Security (COMSEC) material
E4	CORE	Verify cryptographic equipment settings

COMMUNICATIONS SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Coordinate restoral with off-site technicians
E6	CORE	Develop Combat System Training Team (CSTT) scenarios
E5	NON-CORE	Integrate Intelligence, Surveillance, and Reconnaissance (ISR) services (e.g., Global Broadcasting Systems (GBS), Communications Data Link System (CDLS), etc.)
E4	CORE	Load magnetic tape
E4	CORE	Maintain magnetic tape drives
E4	NON-CORE	Perform Information Systems (IS) backups
E4	CORE	Restore computer Information Systems (IS)
E5	CORE	Restore loss of Facilities Control (FACCON)
E6	CORE	Verify communications security policies

CYBERSPACE OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Identify security issues (i.e., protection, aggregation, inter-connectivity)
E5	CORE	Implement security actions

MESSAGE SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Maintain local media and technical libraries

NETWORK ADMINISTRATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Analyze logs
E4	CORE	Back up Information Systems (IS)

NETWORK ADMINISTRATION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Configure network services
E4	CORE	Configure peripherals
E4	CORE	Configure workstation Operating System (OS) software
E5	CORE	Document Information Systems (IS) errors
E4	CORE	Document network outages
E5	CORE	Document off-site technical support actions
E4	CORE	Install network peripherals
E4	NON-CORE	Install network software
E4	CORE	Install Operating Systems (OS)
E4	CORE	Install peripherals
E6	CORE	Maintain network documentation
E7	CORE	Manage audit data
E6	NON-CORE	Manage network system configurations
E6	NON-CORE	Manage network system updates
E4	CORE	Perform disk administration
E4	CORE	Perform file system maintenance
E4	CORE	Perform start up/shut down procedures
E5	NON-CORE	Perform trend analysis (hardware, software, or network)
E4	CORE	Review logs
E4	CORE	Troubleshoot client Operating Systems (OS)
E4	CORE	Troubleshoot workstation application software
E5	NON-CORE	Update network policies
E5	CORE	Verify network system operations

NETWORK MANAGEMENT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Develop disaster recovery contingency plans
E5	CORE	Restore from backups
E4	CORE	Verify backups

NETWORK SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Inventory Information Systems (IS) assets
E5	CORE	Maintain network system databases
E5	CORE	Perform data transfers

Job Title

Cyber Defense Infrastructure Support Specialist

Job Code

002781

Job Family

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

CYBER DEF INFRA SUP SPEC

Short Title (14 Characters)

CD INF SUPSPEC

Pay Plan

Enlisted

Career Field

IT

Other Relationships and Rules

NEC 746A and other NECs as assigned

Job Description

Cyber Defense Infrastructure Support Specialists test, implement, deploy, maintain, review, and administer the infrastructure hardware, software, and documentation that are required to effectively manage network defense resources.

DoD Relationship

Group Title

ADP Computers, General

DoD Code

115000

O*NET Relationship

Occupation Title

Computer Systems Analysts

SOC Code

15-1121.00

Job Family

Computer and Mathematical

Skills

Operation and Control

Technology Design

Management of Material Resources

Critical Thinking

Complex Problem Solving

Systems Analysis

Repairing

Troubleshooting

Writing

Monitoring

Abilities

Deductive Reasoning

Information Ordering

Control Precision

Problem Sensitivity

Inductive Reasoning

Written Comprehension

Written Expression

Category Flexibility

Flexibility of Closure

Manual Dexterity

COMMUNICATIONS SECURITY

Paygrade

Task Type

Task Statements

E5

NON-CORE

Administer client platform securities

E4

CORE

Conduct Emergency Action Plans (EAP)

E4

CORE

Destroy Communication Security (COMSEC) material

E4

NON-CORE

Destroy Key Management Infrastructure (KMI) products

E4

CORE

Handle Communications Security (COMSEC) material

E4

CORE

Inspect security containers

E4

CORE

Maintain physical security of Sensitive Compartmented Information (SCI) Information Systems (IS)

E4

CORE

Report Communications Security (COMSEC) discrepancies

COMMUNICATIONS SYSTEM OPERATIONS

Paygrade

Task Type

Task Statements

E5

NON-CORE

Configure router and switching devices

E5

CORE

Investigate loss of Facilities Control (FACCON)

E4

CORE

Load image software

E4

CORE

Monitor routing and switching devices

E4

NON-CORE

Perform Information Systems (IS) backups

E4

CORE

Restore computer Information Systems (IS)

E5

CORE

Restore loss of Facilities Control (FACCON)

E5

NON-CORE

Troubleshoot router and switching devices

CYBERSPACE OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Analyze organizational security posture trends
E6	NON-CORE	Assess the impact of implementing and sustaining a dedicated cyber defense infrastructure
E5	NON-CORE	Build dedicated cyber defense systems
E6	CORE	Complete network security assessment checklists
E5	NON-CORE	Configure dedicated cyber defense systems
E5	NON-CORE	Configure network firewalls
E7	CORE	Determine patterns of non-compliance (e.g., risk levels, Information Assurance (IA) program effectiveness, etc.)
E6	NON-CORE	Determine potential conflicts with implementation of any cyber defense tools (e.g., tools and signature, testing and optimization)
E5	NON-CORE	Disseminate cyber event information
E5	CORE	Disseminate technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters
E7	NON-CORE	Ensure procedures and guidelines comply with cybersecurity policies
E6	NON-CORE	Evaluate Information Systems Security (ISS)
E7	NON-CORE	Identify critical cyber defense infrastructure and key resources
E4	CORE	Identify Information Systems Security (ISS) violations and vulnerabilities
E7	NON-CORE	Identify Information Technology (IT) security program implications of new technologies or technology upgrades
E4	CORE	Identify security issues (i.e., protection, aggregation, inter-connectivity)
E5	NON-CORE	Implement Information Assurance Vulnerability Alerts (IAVA)
E5	NON-CORE	Implement Information Assurance Vulnerability Bulletins (IAVB)
E6	NON-CORE	Implement Information Systems Security (ISS) policies
E6	CORE	Implement network security applications
E5	NON-CORE	Implement policies and procedures to ensure protection of critical infrastructure
E5	CORE	Implement security actions
E5	NON-CORE	Install dedicated cyber defense systems
E5	NON-CORE	Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware)
E5	CORE	Maintain Information Systems (IS) logs
E4	NON-CORE	Provide technical support to resolve cyber incidents
E7	CORE	Recommend new information technology security requirements
E4	NON-CORE	Remove system viruses
E7	NON-CORE	Report Information Systems Security (ISS) incidents
E7	CORE	Review Information Systems Security (ISS) requirements
E5	NON-CORE	Test dedicated cyber defense systems
E6	NON-CORE	Track audit findings for mitigation actions
E4	CORE	Update computer Information Systems (IS) antivirus definitions

CYBERSPACE OPERATIONS (CONT'D)

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	NON-CORE	Validate migration/installation computer software
E6	NON-CORE	Validate network security improvement actions

MESSAGE SYSTEM OPERATIONS

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Establish Command, Control, Communications, Computers, Combat Systems and Intelligence (C5I) system interconnectivity
E5	CORE	Implement non-repudiation controls
E4	NON-CORE	Install certificates (e.g., security, system, etc.)
E4	CORE	Maintain local media and technical libraries
E7	NON-CORE	Validate unit and command certificates

NETWORK ADMINISTRATION

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	NON-CORE	Administer Information Systems (IS) accounts
E5	CORE	Analyze logs
E4	CORE	Back up Information Systems (IS)
E4	CORE	Configure computer application software
E5	CORE	Configure logs
E4	NON-CORE	Configure network hardware
E5	NON-CORE	Configure network services
E4	CORE	Configure peripherals
E5	NON-CORE	Configure router Access Control Lists (ACL)
E5	NON-CORE	Configure server Operating System (OS) software
E5	NON-CORE	Configure virus scanners
E4	NON-CORE	Configure workstation network connectivity
E4	CORE	Configure workstation Operating System (OS) software
E4	NON-CORE	Construct networks
E5	CORE	Develop Information Systems (IS) Standard Operating Procedures (SOP)
E5	CORE	Document Information Systems (IS) errors
E4	CORE	Document network outages
E5	CORE	Document off-site technical support actions
E5	CORE	Document server outages
E5	NON-CORE	Initialize network servers
E4	NON-CORE	Install network components
E4	CORE	Install network peripherals
E4	NON-CORE	Install network software
E4	CORE	Install Operating Systems (OS)
E4	CORE	Install peripherals
E4	CORE	Isolate infected systems

NETWORK ADMINISTRATION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Maintain Information Systems (IS) servers
E6	CORE	Maintain network documentation
E4	CORE	Maintain network printers
E7	CORE	Manage audit data
E5	NON-CORE	Manage file and folder access
E5	NON-CORE	Manage Information Systems (IS) queues
E5	NON-CORE	Manage Information Systems (IS) servers
E5	NON-CORE	Manage network monitoring software
E6	NON-CORE	Manage network system configurations
E6	NON-CORE	Manage network system updates
E4	CORE	Monitor network equipment status
E4	CORE	Patch information systems
E4	CORE	Perform disk administration
E4	CORE	Perform file system maintenance
E4	CORE	Perform File Transfer Protocol (FTP) functions
E4	CORE	Perform start up/shut down procedures
E5	NON-CORE	Perform trend analysis (hardware, software, or network)
E7	NON-CORE	Plan network restorations
E5	CORE	Prepare network status reports
E4	CORE	Review logs
E4	CORE	Scan for viruses
E4	CORE	Test computer Information Systems (IS)
E4	CORE	Troubleshoot client Operating Systems (OS)
E4	CORE	Troubleshoot file and folder access problems
E4	CORE	Troubleshoot network hardware
E4	CORE	Troubleshoot peripherals
E5	NON-CORE	Troubleshoot server Operating Systems (OS)
E5	CORE	Troubleshoot storage devices
E4	CORE	Troubleshoot workstation application software
E5	NON-CORE	Update network policies
E5	CORE	Verify network system operations

NETWORK MANAGEMENT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Conduct computer software migration
E5	NON-CORE	Configure domain system policies
E7	NON-CORE	Determine network migration and installation potential problems
E7	NON-CORE	Determine network migrations and installation time requirements
E7	CORE	Develop disaster recovery contingency plans

NETWORK MANAGEMENT (CONT'D)

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	NON-CORE	Develop system life cycle plans
E6	NON-CORE	Draft network topologies
E7	NON-CORE	Estimate network migration or installation costs
E6	NON-CORE	Implement domain policies
E7	CORE	Implement Information Systems (IS) equipment and media disposition requirements (e.g., destruction, disposal, transfer, etc.)
E6	NON-CORE	Implement network policies
E5	NON-CORE	Maintain network topologies
E7	NON-CORE	Manage Local Area Network (LAN) architecture
E6	NON-CORE	Manage network system databases
E7	NON-CORE	Manage networking solutions
E7	NON-CORE	Plan network upgrades
E7	NON-CORE	Provide incident details to external organizations (e.g., law enforcement personnel)
E5	CORE	Restore from backups
E4	CORE	Troubleshoot network cabling
E5	NON-CORE	Troubleshoot Wide Area Network (WAN)
E7	CORE	Validate baseline security safeguard installation
E4	CORE	Verify backups

NETWORK SYSTEM OPERATIONS

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Administer network system databases
E5	NON-CORE	Configure virtual environments
E5	NON-CORE	Identify Information Systems anomalies
E7	CORE	Implement network operating procedures
E4	CORE	Inspect Information Systems (IS) (e.g., network components, system hardware, etc.)
E4	CORE	Install Information Systems (IS) components (e.g., system hardware, storage devices, etc.)
E5	NON-CORE	Install servers
E4	CORE	Inventory Information Systems (IS) assets
E7	CORE	Maintain Information Systems (IS) (e.g., Program of Record (POR), authorized, etc.)
E5	CORE	Maintain software application scripts
E5	CORE	Perform data transfer
E5	NON-CORE	Troubleshoot networks (e.g., Integrated Shipboard Network Systems (ISNS), Consolidated Afloat Networks and Enterprise Services (CANES), virtual, etc.)
E4	NON-CORE	Troubleshoot virtual environments
E6	NON-CORE	Write software application scripts

Job Title**Cyber Defense Incident Responder****Job Code****002782****Job Family**

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

CYBER DEF INCIDENT RESPONDER

Short Title (14 Characters)

CD INCNT RSPND

Pay Plan

Enlisted

Career Field

IT

Other Relationships and Rules

NEC 742A and other NECs as assigned

Job Description

Cyber Defense Incident Responders respond to disruptions within the pertinent domain to mitigate immediate and potential threats. Uses mitigation, preparedness, and response and recovery approaches to maximize survival of life, preservation of property, and information security. Investigates and analyzes relevant response activities and evaluates the effectiveness of and improvements to existing practices.

DoD Relationship**Group Title**

ADP Computers, General

DoD Code

115000

O*NET Relationship**Occupation Title**Computer Network Support
Specialists**SOC Code**

15-1152.00

Job Family

Computer and Mathematical

Skills*Operation and Control**Technology Design**Critical Thinking**Complex Problem Solving**Systems Analysis**Management of Material Resources**Writing**Repairing**Monitoring**Troubleshooting***Abilities***Deductive Reasoning**Information Ordering**Control Precision**Problem Sensitivity**Inductive Reasoning**Written Comprehension**Written Expression**Flexibility of Closure**Oral Expression**Reaction Time***COMMUNICATIONS SECURITY****Paygrade**

E5

Task Type

NON-CORE

Task Statements

Administer client platform securities

E4

CORE

Conduct Emergency Action Plans (EAP)

E4

CORE

Destroy Communication Security (COMSEC) material

E4

NON-CORE

Destroy Key Management Infrastructure (KMI) products

E4

CORE

Handle Communications Security (COMSEC) material

E4

CORE

Inspect security containers

E4

CORE

Maintain physical security of Sensitive Compartmented Information (SCI)
Information Systems (IS)

E4

CORE

Report Communications Security (COMSEC) discrepancies

COMMUNICATIONS SYSTEM OPERATIONS**Paygrade**

E5

Task Type

NON-CORE

Task Statements

Configure router and switching devices

E4

CORE

Load image software

E4

CORE

Monitor routing and switching devices

E4

NON-CORE

Perform Information Systems (IS) backups

E5

CORE

Restore loss of Facilities Control (FACCON)

E5

NON-CORE

Troubleshoot router and switching devices

CYBERSPACE OPERATIONS

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Advise leadership of changes affecting the organization's cybersecurity posture
E5	NON-CORE	Analyze Information Systems Security (ISS) posture trends
E5	NON-CORE	Analyze malicious activity
E6	NON-CORE	Assess the impact of implementing and sustaining a dedicated cyber defense infrastructure
E5	NON-CORE	Configure dedicated cyber defense systems
E5	NON-CORE	Configure network firewalls
E7	CORE	Determine patterns of non-compliance (e.g., risk levels, Information Assurance (IA) program effectiveness, etc.)
E5	NON-CORE	Disseminate cyber defense techniques and guidance (e.g., Time Compliance Network Orders (TCNO), concept of operations, net analyst reports, etc.) for the organization
E5	NON-CORE	Disseminate cyber event information
E5	CORE	Disseminate technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters
E7	NON-CORE	Ensure procedures and guidelines comply with cybersecurity policies
E6	NON-CORE	Evaluate Information Systems Security (ISS)
E7	NON-CORE	Evaluate Information Systems Security (ISS) incidents
E7	CORE	Evaluate security improvement actions
E5	NON-CORE	Identify applications and Operating Systems (OS) of a network device based on network traffic
E7	NON-CORE	Identify critical cyber defense infrastructure and key resources
E4	CORE	Identify Information Systems Security (ISS) violations and vulnerabilities
E4	CORE	Identify security issues (i.e., protection, aggregation, inter-connectivity)
E5	NON-CORE	Implement Information Assurance Vulnerability Alerts (IAVA)
E5	NON-CORE	Implement Information Assurance Vulnerability Bulletins (IAVB)
E6	NON-CORE	Implement Information Systems Security (ISS) policies
E6	CORE	Implement network security applications
E5	NON-CORE	Implement policies and procedures to ensure protection of critical infrastructure
E5	CORE	Implement security actions
E5	NON-CORE	Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware)
E5	CORE	Maintain Information Systems (IS) logs
E5	NON-CORE	Perform real-time cyber defense incident handling tasks (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation, etc.)
E4	NON-CORE	Provide technical support to resolve cyber incidents
E7	CORE	Recommend new information technology security requirements
E4	NON-CORE	Remove system viruses
E7	NON-CORE	Report Information Systems Security (ISS) incidents
E7	CORE	Review Information Systems Security (ISS) requirements

CYBERSPACE OPERATIONS (CONT'D)

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Test dedicated cyber defense systems
E6	NON-CORE	Track audit findings for mitigation actions
E4	CORE	Update computer Information Systems (IS) antivirus definitions
E5	NON-CORE	Validate Intrusion Detection System (IDS) alerts

MESSAGE SYSTEM OPERATIONS

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Establish Command, Control, Communications, Computers, Combat Systems and Intelligence (C5I) system interconnectivity
E5	CORE	Implement non-repudiation controls
E4	NON-CORE	Install certificates (e.g., security, system, etc.)
E4	CORE	Maintain local media and technical libraries
E7	NON-CORE	Validate unit and command certificates

NETWORK ADMINISTRATION

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Analyze logs
E4	CORE	Back up Information Systems (IS)
E4	CORE	Configure computer application software
E5	CORE	Configure logs
E4	NON-CORE	Configure network hardware
E5	NON-CORE	Configure network services
E4	CORE	Configure peripherals
E5	NON-CORE	Configure router Access Control Lists (ACL)
E5	NON-CORE	Configure server Operating System (OS) software
E5	NON-CORE	Configure virus scanners
E4	NON-CORE	Configure workstation network connectivity
E4	CORE	Configure workstation Operating System (OS) software
E5	CORE	Develop Information Systems (IS) Standard Operating Procedures (SOP)
E5	CORE	Document Information Systems (IS) errors
E4	CORE	Document network outages
E5	CORE	Document off-site technical support actions
E5	CORE	Document server outages
E6	CORE	Implement remediation plans for identified vulnerabilities
E5	NON-CORE	Initialize network servers
E4	NON-CORE	Install network components
E4	CORE	Install network peripherals
E4	NON-CORE	Install network software
E4	CORE	Install Operating Systems (OS)
E4	CORE	Install peripherals

NETWORK ADMINISTRATION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Isolate infected systems
E6	CORE	Maintain network documentation
E7	CORE	Manage audit data
E5	NON-CORE	Manage file and folder access
E5	NON-CORE	Manage network monitoring software
E6	NON-CORE	Manage network system configurations
E6	NON-CORE	Manage network system updates
E4	CORE	Monitor network equipment status
E4	CORE	Patch Information Systems (IS)
E4	CORE	Perform disk administration
E4	CORE	Perform File Transfer Protocol (FTP) functions
E4	CORE	Perform start up/shut down procedures
E5	NON-CORE	Perform trend analysis (hardware, software, or network)
E7	NON-CORE	Plan network restorations
E5	CORE	Prepare network status reports
E4	CORE	Review logs
E4	CORE	Scan for viruses
E4	CORE	Test computer Information Systems (IS)
E4	CORE	Troubleshoot client Operating Systems (OS)
E4	CORE	Troubleshoot file and folder access problems
E4	CORE	Troubleshoot network hardware
E4	CORE	Troubleshoot peripherals
E5	NON-CORE	Troubleshoot server Operating Systems (OS)
E5	CORE	Troubleshoot storage devices
E4	CORE	Troubleshoot workstation application software
E5	NON-CORE	Update network policies
E5	CORE	Verify network system operations

NETWORK MANAGEMENT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Develop disaster recovery contingency plans
E7	CORE	Develop remediation plans for identified vulnerabilities
E6	NON-CORE	Draft network topologies
E6	NON-CORE	Implement domain policies
E6	NON-CORE	Implement network policies
E5	NON-CORE	Maintain network topologies
E7	NON-CORE	Provide incident details to external organizations (e.g., law enforcement personnel)
E5	NON-CORE	Report Information Systems Security (ISS) posture trends

NETWORK MANAGEMENT (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Restore from backups
E5	NON-CORE	Troubleshoot Wide Area Network (WAN)
E4	CORE	Verify backups

NETWORK SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Inventory Information Systems (IS) assets
E5	CORE	Perform data transfers

Job Title

Vulnerability Assessment Analyst

Job Code

002783

Job Family

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

VULN ASSESSMENT ANALYST

Short Title (14 Characters)

VULN ANALYST

Pay Plan

Enlisted

Career Field

IT

Other Relationships and Rules

NEC 742A and other NECs as assigned

Job Description

Vulnerability Assessment Analysts conduct threat and vulnerability assessments and determine deviations from acceptable configurations or policies. Assesses the level of risk and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

DoD Relationship

Group Title

ADP Computers, General

DoD Code

115000

O*NET Relationship

Occupation Title

Computer Systems Analysts

SOC Code

15-1121.00

Job Family

Computer and Mathematical

Skills

Operation and Control

Critical Thinking

Management of Material Resources

Complex Problem Solving

Monitoring

Writing

Quality Control Analysis

Systems Evaluation

Operations Analysis

Systems Analysis

Abilities

Deductive Reasoning

Information Ordering

Inductive Reasoning

Problem Sensitivity

Control Precision

Written Expression

Written Comprehension

Flexibility of Closure

Perceptual Speed

Oral Expression

COMMUNICATIONS SECURITY

Paygrade

Task Type

Task Statements

E5

NON-CORE

Administer client platform securities

E4

CORE

Conduct Emergency Action Plans (EAP)

E4

CORE

Destroy Communication Security (COMSEC) material

E4

NON-CORE

Destroy Key Management Infrastructure (KMI) products

E6

NON-CORE

Develop Information Systems Security (ISS) plans

E6

NON-CORE

Develop system security certification and accreditation documents

E4

CORE

Handle Communications Security (COMSEC) material

E4

CORE

Inspect security containers

E4

CORE

Maintain physical security of Sensitive Compartmented Information (SCI) Information Systems (IS)

E4

CORE

Report Communications Security (COMSEC) discrepancies

COMMUNICATIONS SYSTEM OPERATIONS

Paygrade

Task Type

Task Statements

E5

NON-CORE

Configure router and switching devices

CYBERSPACE OPERATIONS

Paygrade

Task Type

Task Statements

E5

NON-CORE

Analyze Information Systems Security (ISS) posture trends

E5

NON-CORE

Analyze malicious activity

E5

NON-CORE

Analyze metadata in network traffic

CYBERSPACE OPERATIONS (CONT'D)

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Analyze organizational security posture trends
E6	NON-CORE	Assess the impact of implementing and sustaining a dedicated cyber defense infrastructure
E6	CORE	Complete network security assessment checklists
E5	NON-CORE	Conduct authorized penetration testing on DoD network assets
E7	NON-CORE	Coordinate the protection of critical cyber defense infrastructure and key resources
E7	CORE	Determine patterns of non-compliance (e.g., risk levels, Information Assurance (IA) program effectiveness, etc.)
E6	NON-CORE	Evaluate Information Systems Security (ISS)
E7	NON-CORE	Evaluate Information Systems Security (ISS) incidents
E7	CORE	Evaluate security improvement actions
E5	NON-CORE	Identify applications and Operating Systems (OS) of a network device based on network traffic
E7	NON-CORE	Identify critical cyber defense infrastructure and key resources
E4	CORE	Identify Information Systems Security (ISS) violations and vulnerabilities
E5	NON-CORE	Identify network mapping and Operating System (OS) fingerprinting activities
E4	CORE	Identify security issues (i.e., protection, aggregation, inter-connectivity)
E6	NON-CORE	Implement alternative Information Security (INFOSEC) strategies
E5	NON-CORE	Implement policies and procedures to ensure protection of critical infrastructure
E5	CORE	Implement security actions
E5	NON-CORE	Isolate malicious code
E5	NON-CORE	Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware)
E5	CORE	Maintain Information Systems (IS) logs
E7	NON-CORE	Manage threat or target analysis of adversary's cyber activity information and production of threat information
E5	NON-CORE	Perform cybersecurity assessments
E5	NON-CORE	Perform real-time cyber defense incident handling tasks (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation, etc.)
E4	NON-CORE	Provide technical support to resolve cyber incidents
E5	NON-CORE	Reconstruct a malicious attack or activity based off network traffic
E7	NON-CORE	Report Information Systems Security (ISS) incidents
E5	NON-CORE	Report organizational security posture trends
E7	CORE	Review Information Systems Security (ISS) requirements
E5	NON-CORE	Test dedicated cyber defense systems
E6	NON-CORE	Track audit findings for mitigation actions
E5	NON-CORE	Validate Intrusion Detection System (IDS) alerts
E6	NON-CORE	Validate network security improvement actions

MESSAGE SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Maintain local media and technical libraries

NETWORK ADMINISTRATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Analyze logs
E5	CORE	Document Information Systems (IS) errors
E4	CORE	Document network outages
E5	CORE	Document off-site technical support actions
E5	CORE	Document server outages
E6	CORE	Implement remediation plans for identified vulnerabilities
E4	CORE	Isolate infected systems
E6	CORE	Maintain network documentation
E7	CORE	Manage audit data
E5	NON-CORE	Manage Information Systems (IS) servers
E5	NON-CORE	Manage network monitoring software
E6	NON-CORE	Manage network system configurations
E6	NON-CORE	Manage network system updates
E4	CORE	Monitor network equipment status
E4	CORE	Perform start up/shut down procedures
E5	NON-CORE	Perform trend analysis (hardware, software, or network)
E5	CORE	Prepare network status reports
E4	CORE	Review logs
E4	CORE	Scan for viruses
E4	CORE	Troubleshoot client Operating Systems (OS)
E5	CORE	Verify network system operations

NETWORK MANAGEMENT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Develop remediation plans for identified vulnerabilities
E5	NON-CORE	Maintain network topologies
E7	NON-CORE	Provide incident details to external organizations (e.g., law enforcement personnel)
E5	NON-CORE	Report Information Systems Security (ISS) posture trends
E5	NON-CORE	Troubleshoot Wide Area Network (WAN)
E7	CORE	Validate baseline security safeguard installation

NETWORK SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Inventory Information Systems (IS) assets
E7	CORE	Maintain Information Systems (IS) (e.g., Program of Record (POR), authorized, etc.)
E5	CORE	Maintain software application scripts

NETWORK SYSTEM OPERATIONS (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Perform data transfers
E6	NON-CORE	Write software application scripts

Job Title

Radio Frequency Operator

Job Code

002784

Job Family

Installation, Maintenance, and Repair

NOC

TBD

Short Title (30 Characters)

RADIO FREQUENCY OPERATOR

Short Title (14 Characters)

RF OPERATOR

Pay Plan

Enlisted

Career Field

IT

Other Relationships and Rules

NEC H04A and other NECs as assigned

Job Description

Radio Frequency Operators operate and perform system monitoring, fault isolation and circuit restoration of communications suites in the High Frequency (HF), Ultra High Frequency (UHF), Super High Frequency (SHF), and Extra High Frequency (EHF) frequency spectrums afloat and ashore message centers to include; communication transmission paths, input/output devices, cryptographic devices, interface equipment and patch panels, familiarization with signals, multiplexers, modulators/demodulators, and applicable system transmitters, receivers, couplers and antenna subsystems. Maintains signal quality through the use of circuit and system performance tests, determines point of signal distortion and identifies preventive or corrective action as required. Prepares and maintains all necessary circuit, watch to watch, operational and administrative logs, and ensures accountability of cryptographic publications and associated materials.

DoD Relationship

Group Title

ADP Computers, General

DoD Code

115000

O*NET Relationship

Occupation Title

Telecommunications Equipment Installers and Repairs, Except Line Installers

SOC Code

49-2022.00

Job Family

Installation, Maintenance, and Repair

Skills

Operation and Control
Critical Thinking
Management of Material Resources
Technology Design
Writing
Complex Problem Solving
Monitoring
Systems Evaluation
Systems Analysis
Troubleshooting

Abilities

Deductive Reasoning
Information Ordering
Control Precision
Inductive Reasoning
Written Comprehension
Written Expression
Problem Sensitivity
Category Flexibility
Flexibility of Closure
Oral Expression

COMMUNICATIONS SECURITY

Pavgrade

Task Type

Task Statements

E5	NON-CORE	Administer client platform securities
E6	CORE	Brief communications security roles, responsibilities, obligations, and liabilities
E4	CORE	Conduct Emergency Action Plans (EAP)
E4	CORE	Destroy Communication Security (COMSEC) material
E4	NON-CORE	Destroy Key Management Infrastructure (KMI) products
E6	CORE	Develop Emergency Action Plans (EAP)
E6	NON-CORE	Develop local Communications Security (COMSEC) handling instructions
E5	NON-CORE	Generate local keys
E4	CORE	Handle Communications Security (COMSEC) material
E4	CORE	Identify Communications Security (COMSEC) discrepancies
E6	CORE	Implement Communications Security (COMSEC) changes
E6	CORE	Implement Emergency Action Plans (EAP)
E4	CORE	Inspect security containers
E4	CORE	Inventory Communications Security (COMSEC) materials
E4	CORE	Load Communications Security (COMSEC) equipment

COMMUNICATIONS SECURITY (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Maintain Crypto Ignition Keys (CIK)
E4	CORE	Maintain cryptographic equipment
E4	CORE	Maintain physical security of Sensitive Compartmented Information (SCI) Information Systems (IS)
E5	CORE	Prepare local element Communication Security (COMSEC) reports
E4	CORE	Process Communications Security (COMSEC) changes
E4	CORE	Receive Communications Security (COMSEC) material
E4	CORE	Report Communications Security (COMSEC) discrepancies
E4	CORE	Set up cryptographic equipment
E4	CORE	Set up cryptographic networks
E6	NON-CORE	Transfer custody of Communications Security (COMSEC) material
E4	CORE	Validate Communications Security (COMSEC) material
E4	CORE	Verify cryptographic equipment settings

COMMUNICATIONS SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	NON-CORE	Collect spectrum requirements
E4	CORE	Conduct communications checks
E4	CORE	Conduct Over-The-Air-Rekey (OTAR)
E4	CORE	Conduct Over-The-Air-Transmission (OTAT)
E4	CORE	Configure portable communications systems
E4	CORE	Configure Radio Frequency (RF) systems (e.g., Super High Frequency (SHF), Ultra High Frequency (UHF), Very High Frequency (VHF), Extremely High Frequency (EHF), High Frequency (HF), etc.)
E5	NON-CORE	Configure router and switching devices
E5	NON-CORE	Configure shipboard data rate allocations
E4	CORE	Configure switching equipment (e.g., Automated Single Audio System (ASAS), Automated Network Control Center (ANCC), Tactical Varian Switch (TVS), etc.)
E4	NON-CORE	Configure test equipment (e.g., Spectrum Analyzer, Oscilloscope, Firebird, etc.)
E4	CORE	Connect data links
E5	CORE	Coordinate restoral with off-site technicians
E7	NON-CORE	Deconflict Electromagnetic Interference (EMI)
E6	NON-CORE	Designate circuit frequency assignments
E7	NON-CORE	Determine Joint restricted frequencies
E5	NON-CORE	Determine system configuration requirements
E6	CORE	Develop Combat System Training Team (CSTT) scenarios
E7	NON-CORE	Develop communications policies
E7	NON-CORE	Develop Joint communications electronics operation instructions
E6	NON-CORE	Develop spectrum management plans
E6	NON-CORE	Develop spectrum requirements data call messages
E6	NON-CORE	Develop spectrum requirements summaries

COMMUNICATIONS SYSTEM OPERATIONS (CONT'D)

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Disconnect data links
E6	NON-CORE	Disseminate spectrum management plans
E5	CORE	Document communication reports (e.g., master station log, Communications Spot (COMSPOT), etc.)
E5	CORE	Draft Communications Plans (COMPLANS)
E6	NON-CORE	Draft Operational Task Communications (OPTASK COMMS)
E4	CORE	Ensure proper system operation of Radio Frequency (RF) systems (e.g., Super High Frequency (SHF), Ultra High Frequency (UHF), Very High Frequency (VHF), Extremely High Frequency (EHF), High frequency (HF))
E7	CORE	Evaluate Radio Frequency (RF) communications policies
E4	CORE	Forecast service demands
E5	CORE	Identify electromagnetic interference
E5	CORE	Implement communications plans
E4	NON-CORE	Initialize magnetic tapes drives
E4	CORE	Inspect terminal processors (e.g., Naval Modular Automated Communications System (NAVMACS), Navy Order Wire (NOW), etc.)
E4	NON-CORE	Install electronic Communication Plans (COMPLAN)
E5	NON-CORE	Integrate flight and squadron media
E5	NON-CORE	Integrate Intelligence, Surveillance, and Reconnaissance (ISR) services (e.g., Global Broadcasting Systems (GBS), Communications Data Link System (CDLS), etc.)
E4	NON-CORE	Integrate portable communications systems
E5	CORE	Investigate loss of Facilities Control (FACCON)
E6	NON-CORE	Issue frequency assignments
E4	CORE	Load image software
E4	CORE	Load magnetic tape
E4	CORE	Maintain communication publications
E5	CORE	Maintain communications status boards
E4	CORE	Maintain magnetic tape drives
E4	CORE	Maintain portable communications systems
E5	NON-CORE	Maintain Radio Frequency (RF) circuit configuration files
E4	CORE	Maintain static antennas
E4	CORE	Monitor routing and switching devices
E4	CORE	Perform End of Mission Sanitizations (EOMS)
E4	NON-CORE	Perform Information Systems (IS) backups
E5	NON-CORE	Perform Internet Protocol (IP) shift
E5	NON-CORE	Prepare Satellite Access Requests (SAR)/Gateway Access Request (GAR)/After Action Reports (AAR)/End of Service Report (ESR)
E7	NON-CORE	Report Electromagnetic Interference (EMI)
E4	CORE	Report high priority voice communications
E6	NON-CORE	Resolve Electromagnetic Interference (EMI)

COMMUNICATIONS SYSTEM OPERATIONS (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Restore computer Information Systems (IS)
E5	CORE	Restore loss of Facilities Control (FACCON)
E4	CORE	Set Emission Control (EMCON) conditions
E4	CORE	Set Hazards of Electromagnetic Radiation (Hazards of Electromagnetic Radiation to Ordnance (HERO)/Hazards of Electromagnetic Radiation to Personnel (HERP)) conditions
E5	NON-CORE	Shift message system communication
E4	CORE	Troubleshoot data links
E4	CORE	Troubleshoot portable communications systems
E4	CORE	Troubleshoot Radio Frequency (RF) systems (e.g., Super High Frequency (SHF), Ultra High Frequency (UHF), Very High Frequency (VHF), Extremely High Frequency (EHF), High Frequency (HF), etc.)
E5	NON-CORE	Troubleshoot router and switching devices
E6	NON-CORE	Update spectrum use databases
E6	CORE	Verify communications security policies
E7	NON-CORE	Verify system certifications

CYBERSPACE OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Develop bandwidth management instructions
E7	CORE	Draft Continuity of Operations Program (COOP)
E7	CORE	Forecast service demands
E4	CORE	Identify security issues (i.e., protection, aggregation, inter-connectivity)
E5	NON-CORE	Implement Information Assurance Vulnerability Alerts (IAVA)
E5	NON-CORE	Implement Information Assurance Vulnerability Bulletins (IAVB)
E6	NON-CORE	Implement Information Systems Security (ISS) policies
E5	CORE	Implement security actions
E5	CORE	Maintain Information Systems (IS) logs
E7	NON-CORE	Report Information Systems Security (ISS) incidents
E4	CORE	Update computer Information Systems (IS) antivirus definitions
E6	NON-CORE	Validate migration/installation computer software

MESSAGE SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Complete communication certification checklists
E5	CORE	Configure message processing systems
E4	CORE	Download naval messages via automated systems
E5	CORE	Draft communications spot reports
E5	CORE	Establish Command, Control, Communications, Computers, Combat Systems and Intelligence (C5I) system interconnectivity
E5	CORE	Establish services with communications center

MESSAGE SYSTEM OPERATIONS (CONT'D)

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Establish unit and command certificates
E4	NON-CORE	Install certificates (e.g., security, system, etc.)
E4	CORE	Maintain communication logs
E4	CORE	Maintain communications archives
E4	CORE	Maintain general message files
E4	CORE	Maintain local media and technical libraries
E5	CORE	Manage messaging systems
E5	CORE	Manage operational communications messages
E4	CORE	Monitor message queues
E4	CORE	Monitor message systems
E5	CORE	Perform communications guard shift
E5	CORE	Perform communications shifts
E4	CORE	Perform minimize condition procedures
E4	CORE	Prepare message system status reports
E4	CORE	Process messages (e.g., special handling, American Red Cross (AMCROSS), Situation Reports (SITREPS), etc.)
E5	CORE	Respond to communications spot reports
E4	CORE	Sanitize communication centers
E4	CORE	Validate Naval message formatting
E7	NON-CORE	Validate unit and command certificates

NETWORK ADMINISTRATION

<u>Pavgrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Analyze logs
E4	CORE	Back up Information Systems (IS)
E5	CORE	Configure logs
E5	NON-CORE	Configure router Access Control Lists (ACL)
E5	NON-CORE	Configure server Operating System (OS) software
E5	CORE	Develop Information Systems (IS) Standard Operating Procedures (SOP)
E5	CORE	Document Information Systems (IS) errors
E4	CORE	Document network outages
E5	CORE	Document off-site technical support actions
E6	CORE	Implement remediation plans for identified vulnerabilities
E4	NON-CORE	Implement River City conditions on Information Systems (IS)
E4	CORE	Install Operating Systems (OS)
E5	NON-CORE	Maintain Information Systems (IS) servers
E5	NON-CORE	Manage network monitoring software
E4	CORE	Monitor network equipment status
E4	CORE	Patch Information Systems (IS)

NETWORK ADMINISTRATION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Perform disk administration
E4	CORE	Perform File Transfer Protocol (FTP) functions
E4	CORE	Perform start up/shut down procedures
E5	NON-CORE	Perform trend analysis (hardware, software, or network)
E4	CORE	Respond to customer trouble calls
E4	CORE	Review logs
E4	CORE	Scan for viruses
E4	CORE	Troubleshoot network hardware
E4	CORE	Troubleshoot workstation application software
E5	CORE	Verify network system operations

NETWORK MANAGEMENT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Conduct computer software migration
E7	CORE	Implement Information Systems (IS) equipment and media disposition requirements (e.g., destruction, disposal, transfer, etc.)
E5	CORE	Restore from backups
E4	CORE	Troubleshoot network cabling
E5	NON-CORE	Troubleshoot Wide Area Network (WAN)
E4	CORE	Verify backups

NETWORK SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	NON-CORE	Coordinate Information Systems (IS) backup
E5	CORE	Perform data transfers
E5	CORE	Process customer trouble calls