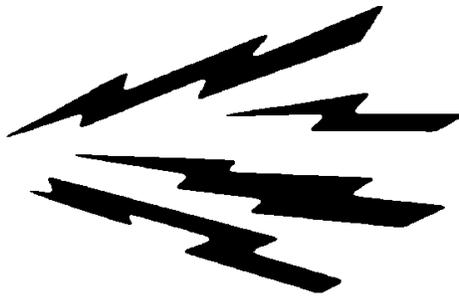


CHAPTER 67



INFORMATION SYSTEMS TECHNICIAN (IT)

NAVPERS 18068-67G

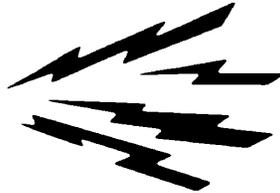
CH-65

Updated: January 2016

TABLE OF CONTENTS
INFORMATION SYSTEMS TECHNICIAN (IT)

SCOPE OF RATING	IT-3
GENERAL INFORMATION	IT-4
INFORMATION TECHNOLOGY NETWORK TECHNICIAN	IT-5
COMMUNICATIONS SECURITY	IT-5
COMMUNICATIONS SYSTEMS OPERATIONS	IT-6
CYBERSPACE OPERATIONS	IT-6
MESSAGE SYSTEMS OPERATIONS	IT-6
NETWORK ADMINISTRATION	IT-7
NETWORK MANAGEMENT	IT-8
NETWORK SYSTEM OPERATIONS	IT-9
INFORMATION TECHNOLOGY SECURITY MANAGER	IT-10
COMMUNICATIONS SECURITY	IT-10
CYBERSPACE OPERATIONS	IT-11
MESSAGE SYSTEM OPERATIONS	IT-12
NETWORK ADMINISTRATION	IT-12
NETWORK MANAGEMENT	IT-13
INFORMATION TECHNOLOGY SECURITY TECHNICIAN	IT-14
COMMUNICATIONS SECURITY	IT-14
COMMUNICATIONS SYSTEMS OPERATIONS	IT-15
CYBERSPACE OPERATIONS	IT-15
MESSAGE SYSTEMS OPERATIONS	IT-16
NETWORK ADMINISTRATION	IT-16
NETWORK MANAGEMENT	IT-17
NETWORK SYSTEM OPERATIONS	IT-17
INFORMATION TECHNOLOGY COMMUNICATION TECHNICIAN	IT-18
COMMUNICATIONS SECURITY	IT-18
COMMUNICATIONS SYSTEMS OPERATIONS	IT-20
CYBERSPACE OPERATIONS	IT-22
MESSAGE SYSTEMS OPERATIONS	IT-22
NETWORK ADMINISTRATION	IT-22
NETWORK MANAGEMENT	IT-23

NAVY ENLISTED OCCUPATIONAL STANDARDS
FOR
INFORMATION SYSTEMS TECHNICIAN (IT)



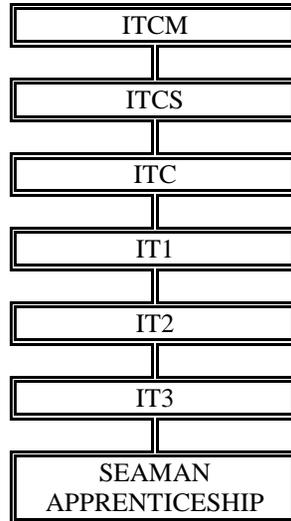
SCOPE OF RATING

Information System Technicians (IT) perform core and specialty functions of communications operations, message processing, and network administration and security; establish, monitor, and maintain Radio Frequency (RF) communications systems; perform spectrum management within an area of responsibility; handle, store, and retrieve incoming and outgoing messages; perform network system administration, maintenance and training; manage, plan and coordinate unit-level information systems security 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

Information Technology Network Technician

Job Code

001414

Job Family
Management

NOC
TBD

Short Title (30 Characters)
INFOR TECHNOLOGY NETWORK TECH

Short Title (14 Characters)
IT NETWRK TECH

Pay Plan
Enlisted

Career Field
IT

Other Relationships and Rules
NECs 2709, 2710, 2720, 2730, 2777, 2778, 2791, 9613, 2781, 2765, 2766, 2792, 2770

Job Description

Information Technology Network Technicians perform core and specialty functions of network administration; install applications and peripherals, troubleshoot computer and network problems, provide assistance with the use of computer hardware and software including printers, applications, and operating systems; conduct system backups and restores; utilize knowledge of database management systems to maintain, administer, test, and implement computer databases; and work with General Service (GENSER), unclassified, and Special Intelligence (SI) systems including administrative, logistical, and tactical data processors in support of strategic, operational, and tactical operations.

DoD Relationship

Group Title ADP Computers, General
DoD Code 115000

O*NET Relationship

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

Skills

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

Abilities

- Deductive Reasoning*
- Information Ordering*
- Control Precision*
- Problem Sensitivity*
- Inductive Reasoning*
- Written Comprehension*
- Written Expression*
- Category Flexibility*
- Mathematical Reasoning*
- Selective Attention*

COMMUNICATIONS SECURITY

Paygrade	Task Type	Task Statements
E4	CORE	Conduct Emergency Action Plans (EAP)
E6	CORE	Develop Emergency Action Plans (EAP)
E4	CORE	Handle Communications Security (COMSEC) material
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) computer Information Systems (IS)
E5	NON-CORE	Manage Key Management Infrastructure (KMI) system configuration
E6	CORE	Monitor Communications Security (COMSEC) platform security
E4	CORE	Prepare local holder Electronic Key Management System (EKMS) reports
E4	CORE	Receive Communications Security (COMSEC) material
E4	CORE	Report Electronic Key Management System (EKMS) discrepancies
E4	CORE	Safeguard classified material

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	CORE	Configure portable communications systems
E5	CORE	Configure router and switching devices
E5	NON-CORE	Integrate flight and squadron media
E5	CORE	Integrate Intelligence, Surveillance, and Reconnaissance (ISR) services (e.g. Global Broadcasting Systems (GBS), Communications Data Link System CDLS), etc.)
E4	CORE	Load image software
E4	NON-CORE	Maintain magnetic tape drives
E4	NON-CORE	Maintain trouble ticket database
E4	CORE	Monitor routing and switching devices
E4	CORE	Restore computer Information Systems (IS)
E4	CORE	Set Emission Control (EMCON) conditions
E5	CORE	Troubleshoot data links
E4	CORE	Utilize test equipment (e.g. specan, o-scope, firebird, etc.)

CYBERSPACE OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	CORE	Evaluate Information Systems Security (ISS) programs
E7	CORE	Evaluate security improvement actions
E5	CORE	Implement security actions
E5	CORE	Maintain security logs
E7	CORE	Manage Information Technology (IT) security priorities
E6	CORE	Validate security improvement actions

MESSAGE SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Apply minimize condition procedures
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
E4	CORE	Install certificates (e.g. security, system, etc.)
E4	CORE	Monitor message queues
E4	CORE	Monitor message systems
E4	CORE	Process messages (e.g. special handling, AMCROSS, SITREPS, etc.)
E4	CORE	Sanitize communication center

NETWORK ADMINISTRATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Administer computer Information System (IS) accounts
E5	CORE	Analyze audit logs
E5	CORE	Back up computer Information Systems (IS)
E5	CORE	Configure audit logs
E4	CORE	Configure computer application software
E4	CORE	Configure external peripherals
E5	CORE	Configure network hardware and software
E5	CORE	Configure print services
E5	CORE	Configure server operating system software
E4	CORE	Configure workstation network connectivity
E4	CORE	Configure workstation Operating System (OS) software
E4	CORE	Construct networks
E5	CORE	Develop computer Information System (IS) Standard Operating Procedures (SOP)
E4	CORE	Document network outages
E5	CORE	Document Operating System (OS) errors
E5	CORE	Document server outages
E5	CORE	Implement River City conditions on computer Information Systems (IS)
E5	CORE	Implement router Access Control Lists (ACL)
E5	CORE	Initialize network servers
E4	CORE	Install external peripherals
E5	CORE	Install network components
E5	CORE	Install network peripherals
E5	CORE	Install network software
E5	CORE	Install Operating Systems (OS)
E5	CORE	Maintain computer Information System (IS) servers
E4	CORE	Maintain network printers
E6	CORE	Manage computer Information System (IS) servers
E5	CORE	Manage file and folder accesses
E6	CORE	Manage network documentation
E6	CORE	Manage network monitoring software
E6	CORE	Manage network system configurations
E6	CORE	Manage network system updates
E4	CORE	Monitor audit logs
E5	CORE	Monitor network equipment
E5	CORE	Monitor network systems
E5	CORE	Perform disk administration
E5	CORE	Perform file system maintenance
E5	CORE	Perform File Transfer Protocol (FTP) functions

E5	CORE	Perform start up/shut down procedures
E6	CORE	Perform trend analysis (hardware, software, or network)
E4	CORE	Perform workstation start up/shut down procedures
E7	CORE	Plan network restorations
E6	CORE	Prepare network status reports
E4	CORE	Respond to customer trouble calls
E4	CORE	Scan for viruses
E5	CORE	Test computer Information Systems (IS)
E4	CORE	Troubleshoot client Operating Systems (OS)
E4	CORE	Troubleshoot external peripherals
E4	CORE	Troubleshoot file and folder access problems
E5	CORE	Troubleshoot network hardware
E5	CORE	Troubleshoot primary storage devices
E5	CORE	Troubleshoot server Operating Systems (OS)
E4	CORE	Troubleshoot workstation application software
E4	CORE	Troubleshoot workstation network connectivity
E5	CORE	Utilize administrative tools
E5	CORE	Utilize computer Information Systems (IS)

NETWORK MANAGEMENT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	CORE	Configure domain system policies
E7	CORE	Determine network migration and installation potential problems
E7	CORE	Determine network migrations and installation time requirements
E6	CORE	Determine network upgrade equipment
E7	CORE	Develop disaster recovery contingency plans
E7	CORE	Develop network plans and policies
E7	CORE	Develop system life cycle plans
E7	NON-CORE	Estimate network migration or installation costs
E7	CORE	Implement Automated Information Systems (AIS) equipment and media disposition requirements (e.g. destruction, disposal, transfer, etc.)
E5	CORE	Implement computer software for migration or installation
E6	CORE	Implement domain policies
E6	CORE	Implement network policies
E7	CORE	Manage Local Area Network (LAN) architecture
E6	CORE	Manage network system databases
E7	CORE	Manage networking solutions
E7	NON-CORE	Oversee information security budget, staffing, and contracting
E5	CORE	Restore from backups
E4	CORE	Troubleshoot network cabling
E5	CORE	Troubleshoot Wide Area Network (WAN) optimization
E5	CORE	Verify backups

NETWORK SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Administer network system databases
E5	CORE	Configure virtual environments
E4	CORE	Configure workstation internal core components
E6	CORE	Coordinate domain backup schedules
E6	CORE	Develop web pages
E5	CORE	Identify information systems anomalies
E7	CORE	Implement network operating procedures
E4	CORE	Inspect computer Information Systems (IS) (e.g. network components, system hardware, etc.)
E4	CORE	Install primary storage devices
E6	CORE	Install servers
E4	CORE	Install workstation internal core components
E4	CORE	Inventory computer Information System (IS) assets
E5	CORE	Maintain computer Information System (IS) logs
E5	CORE	Maintain network system databases
E6	CORE	Maintain software application scripts
E5	CORE	Maintain websites
E7	CORE	Manage Automated Data Processing (ADP) software (e.g. Program of Record (POR), authorized, etc.)
E5	CORE	Monitor customer trouble calls
E5	CORE	Troubleshoot networks (e.g. Integrated Shipboard Network Systems (ISNS), Consolidated Afloat Networks and Enterprise Services (CANES), virtual, etc.)
E5	CORE	Troubleshoot server internal core components (virtual)
E4	CORE	Troubleshoot workstation internal core components (virtual)
E6	CORE	Write software application scripts

Job Title

Information Technology Security Manager

Job Code

001422

Job Family

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

INFOR TECHNOLOGY SECURITY MGR

Short Title (14 Characters)

IT SCTY MGR

Pay Plan

Enlisted

Career Field

IT

Other Relationships and Rules

NECs 2779, 9613

Job Description

Information Technology Security Managers plan, coordinate, and manage unit-level information systems security and integration across platforms, fleets, and services; direct cybersecurity programs and manage and implement information systems security countermeasures and network security programs; ensure proper security and control of Communications Security (COMSEC) systems; develop and review Information Systems Security (ISS) accreditation packages; design, plan, and prepare for network expansions and upgrades; prepare and review checklists for Sensitive Compartmented Information Facility (SCIF) accreditation and periodic inspection; manage administrative functions and security procedures governing the special security program; and coordinate allocation of personnel and financial resources, protection of classified information, and the training of Information Technology Specialists.

DoD Relationship

Group Title

ADP Computers, General

DoD Code

115000

O*NET Relationship

Occupation Title

Information Security Analysts

SOC Code

15-1122.00

Job Family

Computer and Mathematical

Skills

Operation and Control

Critical Thinking

Management of Material Resources

Technology Design

Writing

Complex Problem Solving

Monitoring

Systems Analysis

Coordination

Equipment Selection

Abilities

Deductive Reasoning

Information Ordering

Inductive Reasoning

Control Precision

Written Expression

Problem Sensitivity

Written Comprehension

Category Flexibility

Oral Expression

COMMUNICATIONS SECURITY

Paygrade

E6

Task Type

NON-CORE

Task Statements

Administer access to symmetric Crypto Net Key Management Infrastructure (KMI)

E6

NON-CORE

Administer client platforms Key Management Infrastructure (KMI)

E6

NON-CORE

Administer High Assurance Platforms (HAP)

E6

NON-CORE

Audit Key Management Infrastructure (KMI) management data

E4

CORE

Conduct Emergency Action Plans (EAP)

E6

CORE

Develop Emergency Action Plans (EAP)

E6

CORE

Develop system security certification and accreditation documents

E6

NON-CORE

Establish Key Management Infrastructure (KMI) new product requirements

E4

CORE

Handle Communications Security (COMSEC) material

E6

CORE

Implement Emergency Action Plans (EAP)

E6

NON-CORE

Initialize access to asymmetric cryptologic network

E6

NON-CORE

Initialize Key Management Infrastructure (KMI) devices

E4

CORE

Inspect security containers

E4

CORE

Inventory Communications Security (COMSEC) materials

E4

CORE

Load Communications Security (COMSEC) equipment

E4

CORE

Maintain cryptographic equipment

E6	NON-CORE	Maintain Key Management Infrastructure (KMI) databases
E4	CORE	Maintain physical security of Sensitive Compartmented Information (SCI) computer Information Systems (IS)
E5	NON-CORE	Manage Key Management Infrastructure (KMI) tokens
E6	CORE	Monitor Communications Security (COMSEC) platform security
E5	CORE	Perform personalization of type 1 tokens
E4	CORE	Prepare local holder Electronic Key Management System (EKMS) reports
E4	CORE	Receive Communications Security (COMSEC) material
E5	NON-CORE	Register Key Management Infrastructure (KMI) Operating Account (KOA) agents
E5	NON-CORE	Register Key Management Infrastructure (KMI) users
E4	CORE	Report Electronic Key Management System (EKMS) discrepancies
E4	CORE	Safeguard classified material
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

CYBERSPACE OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Approve new information technology security requirements
E7	NON-CORE	Collaborate with organizational managers to support organizational objectives.
E7	CORE	Determine patterns of non-compliance (e.g. risk levels, Information Assurance (IA) program effectiveness, etc.)
E7	CORE	Develop bandwidth management instructions
E7	CORE	Develop critical infrastructure protection policies and procedures
E7	CORE	Develop domain policies
E7	CORE	Develop Information Systems Security (ISS) policies
E7	CORE	Draft enterprise Continuity Of Operations Program (COOP)
E7	NON-CORE	Ensure procedures and guidelines comply with cybersecurity policies
E7	CORE	Establish Enterprise Information Security Architecture (EISA)
E7	CORE	Evaluate security improvement actions
E7	CORE	Forecast ongoing service demands
E7	CORE	Identify Information Technology (IT) security program implications of new technologies or technology upgrades
E6	CORE	Implement alternative information security strategies
E5	CORE	Implement security actions
E7	CORE	Maintain Information Systems Security (ISS) certification and accreditation documentation
E7	CORE	Manage cybersecurity workforce Information Professional (IP) programs
E7	CORE	Manage electronic spillage
E6	CORE	Manage Information Security (INFOSEC) training and awareness programs
E7	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	CORE	Manage intranet/Department of Defense Information Network (DODIN) security policies
E7	CORE	Manage threat or target analysis of adversary's cyber activity information and production of threat information
E6	NON-CORE	Provide enterprise Information Assurance (IA) and supply chain risk management
E6	CORE	Report Information Security (INFOSEC) compliance
E7	CORE	Report Information Systems Security (ISS) incidents
E7	CORE	Review Information Systems Security (ISS) requirements
E6	CORE	Review security assumption
E6	CORE	Track audit findings for mitigation actions
E6	CORE	Validate migration/installation computer software
E7	CORE	Validate organizational policies, guidelines, procedures, regulations, and laws
E6	CORE	Validate security improvement actions
E7	CORE	Verify acquisitions, procurements, and outsourcing efforts information security requirements
E6	CORE	Verify Information Security (INFOSEC) data sources

MESSAGE SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Apply minimize condition procedures
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
E5	CORE	Establish unit and command certificates
E5	CORE	Implement non-repudiation controls
E4	CORE	Install certificates (e.g. security, system, etc.)
E4	CORE	Monitor message queues
E4	CORE	Monitor message systems
E4	CORE	Prepare message system status reports
E4	CORE	Process messages (e.g. special handling, AMCROSS, SITREPS, etc.)
E4	CORE	Sanitize communication center
E7	CORE	Validate unit and command certificates

NETWORK ADMINISTRATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Analyze audit logs
E4	CORE	Construct networks
E5	CORE	Develop computer Information System (IS) Standard Operating Procedures (SOP)

E5	CORE	Manage computer Information System (IS) queues
E4	CORE	Perform workstation start up/shut down procedures
E7	CORE	Plan network restorations
E4	CORE	Respond to customer trouble calls
E5	CORE	Utilize computer Information Systems (IS)

NETWORK MANAGEMENT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Develop disaster recovery contingency plans
E7	NON-CORE	Evaluate cost-benefit, economic, and risk analysis in decision-making process
E7	NON-CORE	Oversee information security budget, staffing, and contracting
E4	CORE	Troubleshoot network cabling

Job Title

Information Technology Security Technician

Job Code

001427

Job Family

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

INFOR TECHNOLOGY SECURITY TEC

Short Title (14 Characters)

IT SCTY TECH

Pay Plan

Enlisted

Career Field

IT

Other Relationships and Rules

NEC 2780, 9613

Job Description

Information Technology Security Technicians monitor and protect network computer systems by detecting and reporting threats of network intrusion and unauthorized access; protect information from and recover information after loss or damage using backups, virus detection, and recovery software procedures; manage and validate network systems security using hardware, software, and established procedures; utilize Information Assurance (IA) and Computer Network Defense (CND) programs; and perform network accreditations and certifications.

DoD Relationship

Group Title

ADP Computers, General

DoD Code

115000

O*NET Relationship

Occupation Title

Information Security Analysts

SOC Code

15-1122.00

Job Family

Computer and Mathematical

Skills

Operation and Control

Critical Thinking

Technology Design

Management of Material Resources

Writing

Monitoring

Complex Problem Solving

Systems Analysis

Systems Evaluation

Equipment Maintenance

Abilities

Deductive Reasoning

Information Ordering

Control Precision

Inductive Reasoning

Written Expression

Written Comprehension

Problem Sensitivity

Category Flexibility

Oral Expression

COMMUNICATIONS SECURITY

Pavgrade

Task Type

Task Statements

E6

NON-CORE

Administer client platform securities

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) Operating Accounts (KOA)

E6

NON-CORE

Administer Key Management Infrastructure (KMI) user accounts

E6

NON-CORE

Administer token securities

E6

NON-CORE

Audit Key Management Infrastructure (KMI) management data

E6

NON-CORE

Back up Key Management Infrastructure (KMI) accounts

E4

CORE

Conduct Emergency Action Plans (EAP)

E6

CORE

Develop Emergency Action Plans (EAP)

E6

CORE

Develop Information Systems Security (ISS) plans

E6

CORE

Develop local Communications Security (COMSEC) handling instructions

E6

CORE

Develop network security instructions

E4

CORE

Handle Communications Security (COMSEC) material

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
E6	NON-CORE	Maintain Key Management Infrastructure (KMI) databases
E4	CORE	Maintain physical security of Sensitive Compartmented Information (SCI) computer Information Systems (IS)
E5	NON-CORE	Manage Key Management Infrastructure (KMI) system configuration
E5	NON-CORE	Manage Key Management Infrastructure (KMI) tokens
E6	CORE	Monitor Communications Security (COMSEC) platform security
E5	CORE	Perform personalization of type 1 tokens
E4	CORE	Prepare local holder Electronic Key Management System (EKMS) reports
E4	CORE	Receive Communications Security (COMSEC) material
E5	NON-CORE	Register Key Management Infrastructure (KMI) Operating Account (KOA) agents
E5	NON-CORE	Register Key Management Infrastructure (KMI) users
E4	CORE	Report Electronic Key Management System (EKMS) discrepancies
E4	CORE	Safeguard classified material
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	CORE	Configure router and switching devices
E4	NON-CORE	Maintain trouble ticket database

CYBERSPACE OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Complete network security assessment checklists
E6	CORE	Configure network firewalls
E5	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	CORE	Evaluate Information Systems Security (ISS) incidents
E6	CORE	Evaluate Information Systems Security (ISS) programs
E7	CORE	Evaluate security improvement actions
E6	CORE	Evaluate trusted computer security
E5	CORE	Identify Information Systems Security (ISS) violations and vulnerabilities
E5	CORE	Identify security issues (protection, aggregation, inter-connectivity)
E6	CORE	Implement alternative information security strategies
E6	CORE	Implement Information Assurance Vulnerability Alerts (IAVA)
E6	CORE	Implement Information Assurance Vulnerability Bulletins (IAVB)

E6	CORE	Implement Information Systems Security (ISS) policies
E6	CORE	Implement network security applications
E5	CORE	Implement policies and procedures to ensure protection of critical infrastructure
E5	CORE	Implement security actions
E5	CORE	Isolate malicious code
E5	CORE	Maintain security logs
E7	CORE	Manage Information Security (INFOSEC) incident reporting processes
E6	CORE	Manage Information Security (INFOSEC) training and awareness programs
E7	CORE	Manage Information Technology (IT) security priorities
E5	NON-CORE	Post cyber defense techniques and guidance (e.g. Time Compliance Network Orders [TCNO], concept of operations, net analyst reports, etc.) for the organization
E6	NON-CORE	Provide enterprise Information Assurance (IA) and supply chain risk management
E5	CORE	Remove system viruses
E6	CORE	Review security assumption
E6	CORE	Track audit findings for mitigation actions
E4	CORE	Update computer Information System (IS) virus files
E6	CORE	Validate security improvement actions
E6	CORE	Verify Information Security (INFOSEC) data sources

MESSAGE SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Apply minimize condition procedures
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
E4	CORE	Install certificates (e.g. security, system, etc.)
E4	CORE	Monitor message systems
E4	CORE	Process messages (e.g. special handling, AMCROSS, SITREPS, etc.)
E4	CORE	Sanitize communication center

NETWORK ADMINISTRATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Administer computer Information System (IS) accounts
E5	CORE	Analyze audit logs
E5	CORE	Back up computer Information Systems (IS)
E5	CORE	Configure virus scanners
E5	CORE	Develop computer Information System (IS) Standard Operating Procedures (SOP)
E5	CORE	Implement River City conditions on computer Information Systems (IS)
E5	CORE	Maintain computer Information System (IS) servers
E7	CORE	Manage audit data

E5	CORE	Manage computer Information System (IS) queues
E6	CORE	Manage network system updates
E4	CORE	Monitor audit logs
E5	CORE	Monitor network equipment
E5	CORE	Monitor network systems
E5	CORE	Perform file system maintenance
E5	CORE	Perform File Transfer Protocol (FTP) functions
E5	CORE	Perform start up/shut down procedures
E6	CORE	Perform trend analysis (hardware, software, or network)
E4	CORE	Perform workstation start up/shut down procedures
E4	CORE	Respond to customer trouble calls
E4	CORE	Scan for viruses
E4	CORE	Troubleshoot file and folder access problems
E5	CORE	Troubleshoot server Operating Systems (OS)
E5	CORE	Update network policies
E5	CORE	Utilize administrative tools
E5	CORE	Utilize computer Information Systems (IS)

NETWORK MANAGEMENT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Develop disaster recovery contingency plans
E6	CORE	Implement domain policies
E7	NON-CORE	Oversee information security budget, staffing, and contracting
E5	CORE	Restore from backups
E4	CORE	Troubleshoot network cabling
E5	CORE	Verify backups

NETWORK SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Configure virtual environments

Job Title**Information Technology Communication Technician****Job Code****001432****Job Family**

Installation, Maintenance, and Repair

NOC

TBD

Short Title (30 Characters)

INFOR TECHNOLOGY COMM TECH

Short Title (14 Characters)

IT COMM TECH

Pay Plan

Enlisted

Career Field

IT

Other Relationships and Rules

NEC 2301, 2302, 2363, 2378, 9613, 2379

Job Description

Information Technology Communication Technicians perform core and specialty functions of communications operations and message processing; establish, monitor, and maintain Radio Frequency (RF) communications systems; perform spectrum management within an area of responsibility; process and maintain incoming and outgoing messages; perform maintenance and training; manage, plan, and coordinate unit-level information systems and integration across platforms, fleets, and services; and ensure proper security, handling, accounting, reporting, and control of Communications Security (COMSEC) materials, and equipment.

DoD Relationship**Group Title**

ADP Computers, General

DoD Code

115000

O*NET Relationship**Occupation Title**

Telecommunications Equipment Installers and Repairers, Except Line Installers

SOC Code

49-2022.00

Job Family

Installation, Maintenance, and Repair

Skills*Operation and Control**Critical Thinking**Management of Material Resources**Writing**Technology Design**Complex Problem Solving**Troubleshooting**Monitoring**Systems Evaluation**Equipment Selection***Abilities***Deductive Reasoning**Information Ordering**Control Precision**Inductive Reasoning**Written Expression**Problem Sensitivity**Written Comprehension**Oral Expression**Category Flexibility**Selective Attention***COMMUNICATIONS SECURITY****Paygrade**

E6

Task Type

NON-CORE

Task Statements

Administer client platform securities

E6

NON-CORE

Administer Key Management Infrastructure (KMI) Operating Accounts (KOA)

E6

NON-CORE

Administer Key Management Infrastructure (KMI) user accounts

E6

NON-CORE

Administer token securities

E6

NON-CORE

Assign product requestors

E6

NON-CORE

Audit Key Management Infrastructure (KMI) management data

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

E6

CORE

Develop Emergency Action Plans (EAP)

E6

NON-CORE

Endorse Key Management Infrastructure (KMI) adware device

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

E6

NON-CORE

Generate Key Management Infrastructure (KMI) local electronic keys

E6	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
E4	CORE	Inspect security containers
E4	CORE	Inventory Communications Security (COMSEC) materials
E6	NON-CORE	Issue Communication Security (COMSEC) material
E6	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
E6	NON-CORE	Maintain Electronic Key Management System (EKMS) databases
E4	CORE	Maintain physical security of Sensitive Compartmented Information (SCI) computer Information Systems (IS)
E6	CORE	Manage Electronic Key Management System (EKMS) training programs
E6	NON-CORE	Manage Key Management Infrastructure (KMI) Device Distribution Profiles (DDP)
E6	NON-CORE	Manage Key Management Infrastructure (KMI) network connectivity
E6	NON-CORE	Manage Key Management Infrastructure (KMI) production
E6	NON-CORE	Manage Key Management Infrastructure (KMI) system reports
E6	CORE	Monitor Communications Security (COMSEC) platform security
E6	NON-CORE	Order Communications Security (COMSEC) products
E5	CORE	Perform personalization of type 1 tokens
E4	CORE	Prepare local holder Electronic Key Management System (EKMS) reports
E4	CORE	Receive Communications Security (COMSEC) material
E6	NON-CORE	Register Electronic Key Management System (EKMS) users
E5	NON-CORE	Register Key Management Infrastructure (KMI) Operating Account (KOA) agents
E5	NON-CORE	Register Key Management Infrastructure (KMI) users
E6	NON-CORE	Register local Electronic Key Management System (EKMS) elements
E6	CORE	Report Communications Security (COMSEC) compliance
E4	CORE	Report Electronic Key Management System (EKMS) discrepancies
E6	CORE	Review Key Management Infrastructure (KMI) databases
E4	CORE	Safeguard classified material
E4	CORE	Set up cryptographic equipment
E4	CORE	Set up cryptographic networks
E6	NON-CORE	Transfer custody of Communications Security (COMSEC) material
E7	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>
E7	CORE	Collect spectrum requirements
E4	CORE	Conduct communications checks
E4	CORE	Conduct Over-The-Air-Transmission (OTAT) operations
E4	NON-CORE	Configure magnetic tape drives
E5	CORE	Configure portable communications systems
E5	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	CORE	Configure shipboard data rate allocations
E5	CORE	Configure switching equipment (e.g. Automated Single Audio System (ASAS), TVS, Automated Network Control Center (ANCC), etc.)
E5	CORE	Connect data links
E5	CORE	Coordinate restoral with offsite technicians
E7	CORE	Deconflict electromagnetic interference
E6	CORE	Designate circuit frequency assignments
E7	NON-CORE	Determine Joint restricted frequencies
E5	CORE	Determine system configuration requirements
E6	CORE	Develop Combat System Training Team (CSTT) scenarios
E6	CORE	Develop Communications Plans (COMPLANS)
E7	CORE	Develop communications policies
E7	NON-CORE	Develop Joint communications electronics operation instructions
E7	NON-CORE	Develop spectrum management plans
E7	NON-CORE	Develop spectrum requirements data call messages
E7	NON-CORE	Develop spectrum requirements summaries
E5	CORE	Disconnect data links
E7	NON-CORE	Disseminate spectrum management plans
E5	CORE	Document communication reports (e.g. master station log, COMSPOT, C4I, etc.)
E7	CORE	Evaluate Radio Frequency (RF) communications policies
E5	CORE	Identify electromagnetic interference
E6	CORE	Implement communications plans
E4	NON-CORE	Initialize magnetic tapes drives
E5	CORE	Inspect terminal processors (e.g. Naval Modular Automated Communications System (NAVMACS), Navy Order Wire (NOW), etc.)
E4	CORE	Install electronic Communication Plans (COMPLAN)
E5	CORE	Integrate Intelligence, Surveillance, and Reconnaissance (ISR) services (e.g. Global Broadcasting Systems (GBS), Communications Data Link System (CDLS), etc.)
E4	CORE	Integrate portable communications systems (e.g. iridium, Portable Radio Communications (PRC), etc.)

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	NON-CORE	Maintain magnetic tape drives
E5	CORE	Maintain Radio Frequency (RF) circuit configuration files
E5	CORE	Maintain static antennas
E4	NON-CORE	Maintain trouble ticket database
E4	CORE	Monitor portable communications systems (e.g. iridium, Portable Radio communications (PRC), etc.)
E4	CORE	Monitor 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))
E4	CORE	Monitor routing and switching devices
E4	CORE	Perform End of Mission Sanitizations (EOMS)
E4	CORE	Perform Information Systems (IS) backups
E6	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
E4	CORE	Report high priority voice communications
E6	NON-CORE	Resolve electromagnetic interference
E4	CORE	Restore computer Information Systems (IS)
E5	CORE	Restore loss of Facilities Control (FACCON)
E4	CORE	Set Emission Control (EMCON) conditions
E5	CORE	Set Hazards of Electromagnetic Radiation to Ordnance (HERO)/Hazards of Electromagnetic Radiation to Personnel (HERP) conditions
E5	CORE	Shift message system communication
E5	CORE	Troubleshoot data links
E4	CORE	Troubleshoot portable communications systems
E5	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	CORE	Troubleshoot router and switching devices
E5	CORE	Update spectrum use databases
E4	CORE	Utilize test equipment (e.g. specan, o-scope, firebird, etc.)
E6	CORE	Verify communications security policies
E7	CORE	Verify system certifications

CYBERSPACE OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Develop bandwidth management instructions

MESSAGE SYSTEM OPERATIONS

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Apply minimize condition procedures
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
E4	CORE	Install certificates (e.g. security, system, etc.)
E4	CORE	Maintain communications archives
E4	CORE	Maintain general message files
E4	CORE	Maintain local media and technical libraries
E4	CORE	Maintain message logs
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 shifts
E4	CORE	Prepare message system status reports
E4	CORE	Process messages (e.g. special handling, AMCROSS, SITREPS, etc.)
E5	CORE	Respond to communications spot reports
E4	CORE	Sanitize communication center

NETWORK ADMINISTRATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Administer computer Information System (IS) accounts
E5	CORE	Back up computer Information Systems (IS)
E5	CORE	Develop computer Information System (IS) Standard Operating Procedures (SOP)
E6	CORE	Document off-site technical support actions
E5	CORE	Implement River City conditions on computer Information Systems (IS)
E5	CORE	Implement router Access Control Lists (ACL)
E4	CORE	Monitor audit logs
E4	CORE	Perform workstation start up/shut down procedures
E4	CORE	Respond to customer trouble calls

E4	CORE	Troubleshoot external peripherals
E4	CORE	Troubleshoot file and folder access problems
E5	CORE	Utilize computer Information Systems (IS)

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	Troubleshoot network cabling
E5	CORE	Verify backups