CHAPTER 67

INFORMATION SYSTEMS TECHNICIANS, SUBMARINES, ELECTRONIC WARFARE (ITE)

NAVPERS 18068F-67A
Change 102

Updated: April 2025

TABLE OF CONTENTS
INFORMATION SYSTEMS TECHNICIANS, SUBMARINES, ELECTRONIC WARFARE (ITE)

NAVY ENLISTED OCCUPATIONAL STANDARD

FOR

INFORMATION SYSTEMS TECHNICIANS, SUBMARINES, ELECTRONIC WARFARE (ITE)

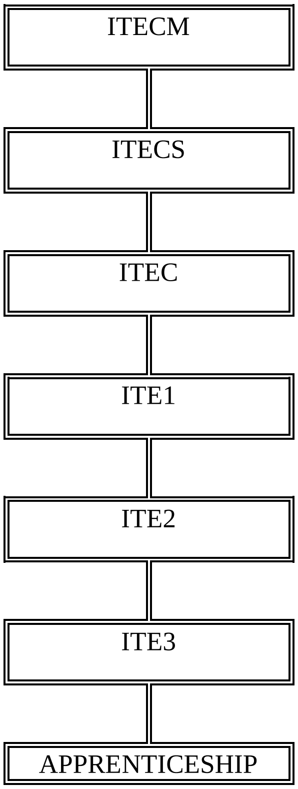
SCOPE OF RATING

Information Systems Technicians, Submarines, Electronic Warfare (ITE) operate and maintain Electronic Intelligence (ELINT)/Electronic Warfare Support (ES) receiving/processing systems and peripheral equipment to provide threat assessments, situational awareness and Indications and Warnings (I&W); aid in the safe operation of the submarine while transiting on the surface or at periscope depth; formulate ES techniques and tactics; perform installations, tests, and preventive and corrective maintenance on electrical and Electronic Warfare (EW) and ancillary systems used for communications, analysis, monitoring, tracking, recognition and identification, ES, and physical security; process and interpret Radio Detection and Ranging (RADAR) emissions for tactical and strategic value; operate, maintain, and repair complex electronic and electro-mechanical equipment; provide safety of forces, I&W, and Information Operations (IO); apply diagnostic and restoration techniques using knowledge of electronic and systems operation theory; provide technical and tactical guidance to Warfare Commanders and National consumers in support of surface, subsurface, air, and special warfare operations; prepare materials providing detailed descriptions of strategic and tactical areas worldwide; provide relevant intelligence to strategic, operational, and tactical level decision-makers; collect, analyze, exploit, and disseminate ELINT in accordance with National and Fleet tasking; advise on capabilities, limitations and equipment conditions of Command, Control, Computer, and Intelligence (C3I) systems; implement and monitor security protocols of C3I systems; implement production control procedures including input/output quality control support of C3I systems; perform organizational level maintenance and repair of C3I systems; operate, maintain, repair and manage Local Area Networks (LAN), Automated Information Systems (AIS), and local databases; operate and maintain General Purpose Test Equipment (GPTE) and auxiliary equipment; and ensure the proper security, handling, accounting, reporting, and control of Communications Security (COMSEC) materials, systems, and equipment.

This Occupational Standard is 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	Job Code
Electronic Warfare Technician	**002786**

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Protective Service	TBD	ELECTRONIC WARFARE TECHNICIAN	EW TECH

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	ITE	NEC TXXX series and other NECs as assigned

Job Description

Electronic Warfare Technicians operate and maintain Electronic Warfare (EW) system equipment to perform advanced analysis, conduct fusion analysis of Signals of Interests (SOI) from platform emitters, and exploit SOI to identify, locate and report hazards and threat platforms; perform advanced electronic intelligence (ELINT) and communication intelligence (COMINT) analysis that include managing submarine electronic support equipment and tasking, analyzing ELINT and COMINT SOI, analyzing ELINT and COMINT using national databases, classifying platforms, and disseminating ELINT and COMINT information; provide current intelligence and knowledge of National Overhead Systems (NOS) software, databases, and platform identification on all submarine platforms while both underway and in-port for mission planning and execution; perform core and specialty functions of network administration within physical and virtual environments; troubleshoot and assist with the use of computer hardware and software including printers and software applications; conduct system backups and restores; install applications and peripherals; 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; utilize Information Assurance (IA) and Computer Network Defense (CND) programs; conduct threat and vulnerability assessments; perform network accreditations and certifications; and receive, inventory, load, and destroy Communications Security (COMSEC) material.

DoD Relationship

Group Title	DoD Code
ADP Computers, General	115000

O*NET Relationship

Occupation Title	SOC Code	Job Family
Intelligence Analysts	33-3021.06	Protective Service

Skills

Operation and Control

Management of Material Resources

Critical Thinking

Quality Control Analysis

Monitoring

Operation Monitoring

Equipment Maintenance

Judgment and Decision Making

Systems Analysis

Coordination

Abilities

Deductive Reasoning

Information Ordering

Problem Sensitivity

Inductive Reasoning

Written Comprehension

Perceptual Speed

Flexibility of Closure

Time Sharing

Mathematical Reasoning

Speed of Closure

ADMINISTRATION

Paygrade	Task Type	Task Statements
E5	CORE	Construct Order of Battle (OOB)
E4	CORE	Determine adversary capabilities and limitations
E4	CORE	Determine Intelligence Community (IC) databases
E5	CORE	Determine jamming sources
E5	CORE	Develop Electronic Warfare Support (ES) search plans (i.e., Radio Detection and Ranging (RADAR), communications)
E5	CORE	Develop operational products based on Pattern of Life (PoL)
E5	CORE	Disseminate Electronic Warfare Support (ES) data and reports
E5	NON-CORE	Draft Naval messages
E5	CORE	Generate Requests for Information (RFI)
E5	CORE	Maintain network documentation (e.g., Systems Authorization Access Request-Navy (SAAR-N), Privileged Access Agreement (PAA), etc.)
E4	CORE	Maintain Top Secret (TS)/Sensitive Compartmented Information (SCI) accountability
E5	CORE	Prioritize mission threats
E4	CORE	Report Electromagnetic Interference (EMI)

ADMINISTRATION (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Report jamming sources
E5	CORE	Search Electronic Intelligence (ELINT) databases
E6	CORE	Supervise signals analysis and reporting
E5	CORE	Update computer configuration documentation (e.g., AN/BLQ-10 workstations and servers, Submarine Local Area Network (SUBLAN)/ Consolidated Afloat Network and Enterprise Services (CANES), etc.)
E6	CORE	Validate Electronic Warfare Support (ES) logs
E4	NON-CORE	Verify Emissions Control (EMCON) conditions are in effect

COMMUNICATIONS SECURITY (COMSEC)

Paygrade	Task Type	Task Statements
E4	CORE	Destroy Communication Security (COMSEC) materials
E4	CORE	Identify Communications Security (COMSEC) discrepancies
E4	CORE	Inventory Communications Security (COMSEC) materials
E4	CORE	Load Communications Security (COMSEC) equipment
E4	CORE	Load Communications Security (COMSEC) materials
E6	NON-CORE	Monitor Communications Security (COMSEC) platform security
E4	CORE	Receive Communications Security (COMSEC) materials
E4	CORE	Store Communications Security (COMSEC) material

CYBER SECURITY

Paygrade	Task Type	Task Statements
E4	CORE	Analyze Information Systems Security (ISS) requirements
E5	CORE	Evaluate system vulnerabilities (e.g., Electronic Warfare (EW), AN/BLQ-10, etc.)
E4	CORE	Maintain Information Systems Security (ISS) logs
E7	CORE	Report Information Security (INFOSEC) compliance
E4	CORE	Report Information Systems Security (ISS) incidents
E4	CORE	Report Information Systems Security (ISS) violations
E4	CORE	Report Information Systems Security (ISS) vulnerabilities
E5	NON-CORE	Update network security tools

ELECTRONIC WARFARE SYSTEMS OPERATIONS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze Electromagnetic (EM) spectrum
E4	CORE	Analyze national systems broadcast data (e.g., Integrated Broadcast System/Common Integrated Broadcast (IBS/CIB), etc.)
E5	CORE	Analyze operational environment for Radio Frequency (RF) systems frequency requirements
E5	CORE	Analyze Signals of Interest (SOI)
E4	CORE	Analyze signals using Electronic Warfare Support (ES) systems (e.g., Pulse Repetition Intervals (PRI), pulse width, Pulse Repetition Frequency (PRF), etc.)
E4	CORE	Assess Indication & Warning (I&W) threats
E5	CORE	Calculate Radio Detection and Ranging (RADAR) parameters (e.g., Maximum Unambiguous Ranges (MUR), minimum range, etc.)

ELECTRONIC WARFARE SYSTEMS OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Conduct Electronic Warfare Support (ES) systems operations
E5	CORE	Conduct Pattern of Life (PoL) analysis
E5	NON-CORE	Conduct Radio Frequency (RF) propagation modeling
E5	CORE	Conduct Specific Emitter Identification (SEI) collections (e.g., Unintentional Modulation on Pulse (UMOP), etc.)
E4	CORE	Configure Common Integrated Broadcast (CIB) radio receiving equipment
E4	CORE	Configure Electronic Warfare Support (ES) systems
E4	CORE	Configure software-based analysis tools
E5	CORE	Configure systems for optimal signals collection
E4	CORE	Correlate national systems data to platform
E4	CORE	Demodulate Radio Frequency (RF) signals
E4	CORE	Determine jamming sources
E4	CORE	Determine Radio Detection and Ranging (RADAR) systems capabilities
E4	CORE	Determine target source utilizing Unintentional Modulation on Pulse (UMOP)
E4	CORE	Employ cyclic routine
E5	CORE	Evaluate emitter signal quality
E5	CORE	Evaluate mission threats
E4	CORE	Identify Electromagnetic Interference (EMI)
E5	CORE	Mitigate Electromagnetic Interference (EMI)
E5	CORE	Monitor own force for electronic emissions
E5	CORE	Perform fusion analysis
E5	CORE	Perform modulation analysis (e.g., Pulse Repetition Frequency (PRF), Amplitude Modulation on Pulse (AMOP), etc.)
E5	CORE	Perform Operational Electronic Intelligence (OPELINT) analysis (e.g., situational Awareness, etc.)
E4	CORE	Perform Pre-Planned Responses (PPR)
E4	CORE	Perform Radio Direction Findings (RDF) of Signals of Interest (SOI)
E5	CORE	Perform waveform analysis
E5	CORE	Perform wavelength to frequency conversions
E5	CORE	Predict equipment performance characteristics based on atmospheric data
E5	CORE	Provide tactical communication intercept support

EQUIPMENT MAINTENANCE

Paygrade	Task Type	Task Statements
E4	CORE	Analyze network audit logs
E5	NON-CORE	Implement Emissions Control (EMCON)
E5	NON-CORE	Recover systems using Disaster Recovery Plan (DRP)
E5	CORE	Repair Electronic Warfare Support (ES) systems
E5	CORE	Repair mast and antenna systems

EQUIPMENT MAINTENANCE (CONT'D)

Paygrade	**Task Type**	**Task Statements**
E4	CORE	Review equipment status for proper operation
E5	CORE	Supervise construction of emitter libraries
E6	CORE	Supervise mast and antenna maintenance
E5	CORE	Troubleshoot Electronic Warfare Support (ES) systems
E5	NON-CORE	Troubleshoot Identification, Friend or Foe (IFF) systems
E5	CORE	Troubleshoot mast and antenna systems
E5	CORE	Validate system Radio Frequency (RF) distribution paths

NETWORK MANAGEMENT

Paygrade	**Task Type**	**Task Statements**
E4	CORE	Apply Information Systems (IS) file and folder permissions
E5	CORE	Manage network databases (e.g., SQL, Oracle, Microsoft (MS) Access, etc.)
E5	CORE	Repair databases (e.g., SQL, Oracle, Microsoft (MS) Access, etc.)
E5	NON-CORE	Troubleshoot virtual network environments

NETWORK OPERATIONS

Paygrade	**Task Type**	**Task Statements**
E4	CORE	Administer computer Information System (IS) user accounts
E4	CORE	Analyze Information System (IS) trends (e.g., hardware, software, network, etc.)
E5	CORE	Troubleshoot databases (e.g., SQL, Oracle, Microsoft (MS) Access, etc.)
E5	CORE	Verify delivered Information Systems (IS) functionality (i.e., System Operational Verification Test (SOVT))
E5	CORE	Verify delivered network components functionality (i.e., System Operational Verification Test (SOVT))
E5	CORE	Verify delivered system hardware functionality (i.e., System Operational Verification Test (SOVT))

Job Title	**Job Code**
Electronic Warfare Manager	**002787**

Job Family	**NOC**	**Short Title (30 Characters)**	**Short Title (14 Characters)**
Business and Financial Operations	TBD	ELECTRONIC WARFARE MANAGER	EW MANAGER

Pay Plan	**Career Field**	**Other Relationships and Rules**
Enlisted	ITE	NEC TXXX series and other NECs as assigned

Job Description

Electronic Warfare Managers assess Electronic Warfare (EW) system training, audit EW records, and coordinate EW system maintenance; coordinate EW equipment modifications; develop EW employment plans and shipboard instructions; prepare EW emergency destruction plans; supervise EW watchstanders in advanced Electronic Intelligence (ELINT) and Communication Intelligence (COMINT) analysis that include managing submarine electronic support equipment and tasking, analyzing ELINT and COMINT Signals of Interest (SOI), analyzing ELINT and COMINT using national databases, classifying platforms and disseminating ELINT and COMINT information; provide current intelligence and knowledge of National Overhead Systems (NOS) software, databases and platform identification on all submarine platforms while both underway and in-port for mission planning and execution; serve as principal advisor to the Commanding Officer in all aspects of EW, Electronic Operations (EO), Indication & Warning (I&W) Operations, EW capabilities, EW offensive and defensive tactics, EW manning concerns, training, and electromagnetic and communication spectrum management; supervise the storage, receipt, load, and destruction of Communication Security (COMSEC) material; monitor maintenance quality control; coordinate and manage unit-level Information Systems (IS) security and integration across platforms, fleets, and services; approve policies for and direct Information Assurance (IA) programs; manage and implement IS security countermeasures and network security programs; develop and review IS security assessment and authorization packages; plan and prepare for network expansions and upgrades; manage administrative functions and security procedures governing the special security program; serve as unit Information Systems Security Manager (ISSM) or unit Systems Administrator (SYSADMIN).

DoD Relationship		**O*NET Relationship**		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
ADP Computers, General	115000	Management Analysts	13-1111.00	Business and Financial Operations

Skills	**Abilities**
Management of Material Resources	*Deductive Reasoning*
Operation and Control	*Information Ordering*
Critical Thinking	*Problem Sensitivity*
Quality Control Analysis	*Written Comprehension*
Coordination	*Inductive Reasoning*
Judgment and Decision Making	*Perceptual Speed*
Monitoring	*Flexibility of Closure*
Systems Evaluation	*Time Sharing*
Operation Monitoring	*Written Expression*
Systems Analysis	*Speed of Closure*

ADMINISTRATION

Paygrade	**Task Type**	**Task Statements**
E7	NON-CORE	Approve Information Systems (IS) Standard Operating Procedures (SOP)
E5	CORE	Construct Order of Battle (OOB)
E6	CORE	Coordinate Electronic Warfare (EW) test range runs
E6	CORE	Coordinate System Operation Verification Testing (SOVT)
E4	CORE	Determine adversary capabilities and limitations
E4	CORE	Determine Intelligence Community (IC) databases
E5	CORE	Determine jamming sources
E7	CORE	Develop Electronic Warfare (EW) tactics
E5	CORE	Develop Electronic Warfare Support (ES) search plans (i.e., Radio Detection and Ranging (RADAR), communications)
E7	NON-CORE	Develop joint service Electronic Warfare (EW) plans
E5	CORE	Develop operational products based on Pattern of Life (PoL)
E5	CORE	Disseminate Electronic Warfare Support (ES) data and reports

ADMINISTRATION (CONT'D)

Paygrade	Task Type	Task Statements
E5	NON-CORE	Draft Naval messages
E6	CORE	Evaluate Electronic Warfare (EW) Measures of Effectiveness (MOE)
E5	CORE	Generate Requests for Information (RFI)
E6	NON-CORE	Interpret test and evaluation range results
E6	NON-CORE	Maintain Information Systems Security (ISS) assessment and authorization documentation
E5	CORE	Maintain network documentation (e.g., Systems Authorization Access Request-Navy (SAAR-N), Privileged Access Agreement (PAA), etc.)
E4	CORE	Maintain Top Secret (TS)/Sensitive Compartmented Information (SCI) accountability
E5	CORE	Prioritize mission threats
E4	CORE	Report Electromagnetic Interference (EMI)
E4	CORE	Report jamming sources
E5	CORE	Search Electronic Intelligence (ELINT) databases
E6	CORE	Supervise Pre-Planned Responses (PPR) executions
E6	CORE	Supervise signals analysis and reporting
E5	CORE	Update computer configuration documentation (e.g., AN/BLQ-10 workstations and servers, Submarine Local Area Network (SUBLAN)/ Consolidated Afloat Network and Enterprise Services (CANES), etc.)
E6	CORE	Validate Electronic Warfare Support (ES) logs
E4	NON-CORE	Verify Emissions Control (EMCON) conditions are in effect

COMMUNICATIONS SECURITY (COMSEC)

Paygrade	Task Type	Task Statements
E4	CORE	Destroy Communication Security (COMSEC) materials
E4	CORE	Identify Communications Security (COMSEC) discrepancies
E4	CORE	Inventory Communications Security (COMSEC) materials
E4	CORE	Load Communications Security (COMSEC) equipment
E4	CORE	Load Communications Security (COMSEC) materials
E6	NON-CORE	Monitor Communications Security (COMSEC) platform security
E4	CORE	Receive Communications Security (COMSEC) materials
E4	CORE	Store Communications Security (COMSEC) material

CYBER SECURITY

Paygrade	Task Type	Task Statements
E4	CORE	Analyze Information Systems Security (ISS) requirements
E6	NON-CORE	Evaluate Information Systems Security (ISS) incidents
E6	NON-CORE	Evaluate Information Systems Security (ISS) violations
E6	NON-CORE	Evaluate Information Systems Security (ISS) vulnerabilities
E5	CORE	Evaluate system vulnerabilities (e.g., Electronic Warfare (EW), AN/BLQ-10, etc.)
E7	NON-CORE	Implement Information Systems Security (ISS) directives (e.g., policies, plans, instructions, Standard Operating Procedures (SOP), etc.)
E4	CORE	Maintain Information Systems Security (ISS) logs
E7	NON-CORE	Manage Information Security (INFOSEC) system programs

CYBER SECURITY (CONT'D)

Paygrade	Task Type	Task Statements
E7	CORE	Report Information Security (INFOSEC) compliance
E4	CORE	Report Information Systems Security (ISS) incidents
E4	CORE	Report Information Systems Security (ISS) violations
E4	CORE	Report Information Systems Security (ISS) vulnerabilities
E5	NON-CORE	Update network security tools

ELECTRONIC WARFARE SYSTEMS OPERATIONS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze Electromagnetic (EM) spectrum
E4	CORE	Analyze national systems broadcast data (e.g., Integrated Broadcast System/Common Integrated Broadcast (IBS/CIB), etc.)
E5	CORE	Analyze operational environment for Radio Frequency (RF) systems frequency requirements
E5	CORE	Analyze Signals of Interest (SOI)
E4	CORE	Analyze signals using Electronic Warfare Support (ES) systems (e.g., Pulse Repetition Intervals (PRI), pulse width, Pulse Repetition Frequency (PRF), etc.)
E4	CORE	Assess Indication & Warning (I&W) threats
E5	CORE	Calculate Radio Detection and Ranging (RADAR) parameters (e.g., Maximum Unambiguous Ranges (MUR), minimum range, etc.)
E4	CORE	Conduct Electronic Warfare Support (ES) systems operations
E5	CORE	Conduct Pattern of Life (PoL) analysis
E5	NON-CORE	Conduct Radio Frequency (RF) propagation modeling
E5	CORE	Conduct Specific Emitter Identification (SEI) collections (e.g., Unintentional Modulation on Pulse (UMOP), etc.)
E4	CORE	Configure Common Integrated Broadcast (CIB) radio receiving equipment
E4	CORE	Configure Electronic Warfare Support (ES) systems
E4	CORE	Configure software-based analysis tools
E5	CORE	Configure systems for optimal signals collection
E4	CORE	Correlate national systems data to platform
E4	CORE	Demodulate Radio Frequency (RF) signals
E4	CORE	Determine jamming sources
E4	CORE	Determine Radio Detection and Ranging (RADAR) systems capabilities
E4	CORE	Determine target source utilizing Unintentional Modulation on Pulse (UMOP)
E6	NON-CORE	Develop Embedded Training Device (ETD) scenarios
E4	CORE	Employ cyclic routine
E5	CORE	Evaluate emitter signal quality
E5	CORE	Evaluate mission threats
E4	CORE	Identify Electromagnetic Interference (EMI)
E6	CORE	Manage Electronic Warfare (EW) operations
E5	CORE	Mitigate Electromagnetic Interference (EMI)
E5	CORE	Monitor own force for electronic emissions
E5	CORE	Perform fusion analysis

ELECTRONIC WARFARE SYSTEMS OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E5	CORE	Perform modulation analysis (e.g., Pulse Repetition Frequency (PRF), Amplitude Modulation on Pulse (AMOP), etc.)
E5	CORE	Perform Operational Electronic Intelligence (OPELINT) analysis (e.g., situational Awareness, etc.)
E4	CORE	Perform Pre-Planned Responses (PPR)
E4	CORE	Perform Radio Direction Findings (RDF) of Signals of Interest (SOI)
E5	CORE	Perform waveform analysis
E5	CORE	Perform wavelength to frequency conversions
E5	CORE	Predict equipment performance characteristics based on atmospheric data
E5	CORE	Provide tactical communication intercept support
E6	NON-CORE	Validate Embedded Training Device (ETD) scenarios

EQUIPMENT MAINTENANCE

Paygrade	Task Type	Task Statements
E4	CORE	Analyze network audit logs
E6	CORE	Coordinate Electronic Warfare (EW) equipment installation
E6	CORE	Coordinate Electronic Warfare (EW) equipment removal
E5	NON-CORE	Implement Emissions Control (EMCON)
E5	NON-CORE	Recover systems using Disaster Recovery Plan (DRP)
E5	CORE	Repair Electronic Warfare Support (ES) systems
E5	CORE	Repair mast and antenna systems
E4	CORE	Review equipment status for proper operation
E5	CORE	Supervise construction of emitter libraries
E6	CORE	Supervise mast and antenna maintenance
E5	CORE	Troubleshoot Electronic Warfare Support (ES) systems
E5	NON-CORE	Troubleshoot Identification, Friend or Foe (IFF) systems
E5	CORE	Troubleshoot mast and antenna systems
E6	CORE	Validate mission plans
E5	CORE	Validate system Radio Frequency (RF) distribution paths

NETWORK MANAGEMENT

Paygrade	Task Type	Task Statements
E4	CORE	Apply Information Systems (IS) file and folder permissions
E6	NON-CORE	Coordinate catastrophic disaster recoveries
E5	CORE	Manage network databases (e.g., SQL, Oracle, Microsoft (MS) Access, etc.)
E6	CORE	Plan network restorations
E5	CORE	Repair databases (e.g., SQL, Oracle, Microsoft (MS) Access, etc.)
E5	NON-CORE	Troubleshoot virtual network environments

NETWORK OPERATIONS

Paygrade	Task Type	Task Statements
E4	CORE	Administer computer Information System (IS) user accounts
E4	CORE	Analyze Information System (IS) trends (e.g., hardware, software, network, etc.)

NETWORK OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E5	CORE	Troubleshoot databases (e.g., SQL, Oracle, Microsoft (MS) Access, etc.)
E5	CORE	Verify delivered Information Systems (IS) functionality (i.e., System Operational Verification Test (SOVT))
E5	CORE	Verify delivered network components functionality (i.e., System Operational Verification Test (SOVT))
E5	CORE	Verify delivered system hardware functionality (i.e., System Operational Verification Test (SOVT))

Job Title	**Job Code**
Electronic Warfare Specialist	**002792**

Job Family	**NOC**	**Short Title (30 Characters)**	**Short Title (14 Characters)**
Architecture and Engineering	TBD	ELECTRONIC WARFARE SPECIALIST	EW SPEC

Pay Plan	**Career Field**	**Other Relationships and Rules**
Enlisted	ITE	NEC TXXX series and other NECs as assigned

Job Description

Electronic Warfare Specialists operate Electronic Warfare (EW) system equipment to perform basic analysis and exploit Signals of Interest (SOI) to identify, locate and report hazards and threat platforms; perform core and specialty functions of network administration within physical and virtual environments; troubleshoot and assist with the use of computer hardware and software including printers and software applications; conduct system backups and restores; install applications and peripherals; 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; utilize Information Assurance (IA) and Computer Network Defense (CND) programs; perform network accreditations and certifications; and receive, inventory, load, and destroy Communications Security (COMSEC) material.

DoD Relationship | **O*NET Relationship**

Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
ADP Computers, General	115000	Electro-Mechanical and Mechatronics Technologists and Technicians	17-3024.00	Architecture and Engineering

Skills	**Abilities**
Operation and Control	*Deductive Reasoning*
Management of Material Resources	*Information Ordering*
Critical Thinking	*Inductive Reasoning*
Quality Control Analysis	*Problem Sensitivity*
Monitoring	*Written Comprehension*
Operation Monitoring	*Perceptual Speed*
Coordination	*Time Sharing*
Complex Problem Solving	*Flexibility of Closure*
Mathematics	*Speed of Closure*
Reading Comprehension	*Mathematical Reasoning*

ADMINISTRATION

Paygrade	**Task Type**	**Task Statements**
E4	CORE	Determine adversary capabilities and limitations
E4	CORE	Determine Intelligence Community (IC) databases
E5	CORE	Disseminate Electronic Warfare Support (ES) data and reports
E5	CORE	Maintain network documentation (e.g., Systems Authorization Access Request-Navy (SAAR-N), Privileged Access Agreement (PAA), etc.)
E4	CORE	Report Electromagnetic Interference (EMI)
E4	NON-CORE	Verify Emissions Control (EMCON) conditions are in effect

COMMUNICATIONS SECURITY (COMSEC)

Paygrade	**Task Type**	**Task Statements**
E4	CORE	Destroy Communication Security (COMSEC) materials
E4	CORE	Identify Communications Security (COMSEC) discrepancies
E4	CORE	Inventory Communications Security (COMSEC) materials
E4	CORE	Load Communications Security (COMSEC) equipment
E4	CORE	Load Communications Security (COMSEC) materials
E6	NON-CORE	Monitor Communications Security (COMSEC) platform security

COMMUNICATIONS SECURITY (COMSEC) (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Receive Communications Security (COMSEC) materials
E4	CORE	Store Communications Security (COMSEC) material

CYBER SECURITY

Paygrade	Task Type	Task Statements
E4	CORE	Analyze Information Systems Security (ISS) requirements
E4	CORE	Maintain Information Systems Security (ISS) logs
E4	CORE	Report Information Systems Security (ISS) incidents
E4	CORE	Report Information Systems Security (ISS) violations
E4	CORE	Report Information Systems Security (ISS) vulnerabilities
E5	NON-CORE	Update network security tools

ELECTRONIC WARFARE SYSTEMS OPERATIONS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze Electromagnetic (EM) spectrum
E4	CORE	Analyze national systems broadcast data (e.g., Integrated Broadcast System/Common Integrated Broadcast (IBS/CIB), etc.)
E5	CORE	Analyze operational environment for Radio Frequency (RF) systems frequency requirements
E5	CORE	Analyze Signals of Interest (SOI)
E4	CORE	Analyze signals using Electronic Warfare Support (ES) systems (e.g., Pulse Repetition Intervals (PRI), pulse width, Pulse Repetition Frequency (PRF), etc.)
E4	CORE	Assess Indication & Warning (I&W) threats
E5	CORE	Calculate Radio Detection and Ranging (RADAR) parameters (e.g., Maximum Unambiguous Ranges (MUR), minimum range, etc.)
E4	CORE	Conduct Electronic Warfare Support (ES) systems operations
E4	CORE	Configure Common Integrated Broadcast (CIB) radio receiving equipment
E4	CORE	Configure Electronic Warfare Support (ES) systems
E4	CORE	Configure software-based analysis tools
E4	CORE	Correlate national systems data to platform
E4	CORE	Demodulate Radio Frequency (RF) signals
E4	CORE	Determine jamming sources
E4	CORE	Determine Radio Detection and Ranging (RADAR) systems capabilities
E4	CORE	Determine target source utilizing Unintentional Modulation on Pulse (UMOP)
E4	CORE	Employ cyclic routine
E5	CORE	Evaluate emitter signal quality
E5	CORE	Evaluate mission threats
E4	CORE	Identify Electromagnetic Interference (EMI)
E5	CORE	Mitigate Electromagnetic Interference (EMI)
E5	CORE	Monitor own force for electronic emissions
E5	CORE	Perform fusion analysis
E5	CORE	Perform modulation analysis (e.g., Pulse Repetition Frequency (PRF), Amplitude Modulation on Pulse (AMOP), etc.)

ELECTRONIC WARFARE SYSTEMS OPERATIONS (CONT'D)

Paygrade	**Task Type**	**Task Statements**
E5	CORE	Perform Operational Electronic Intelligence (OPELINT) analysis (e.g., situational Awareness, etc.)
E4	CORE	Perform Pre-Planned Responses (PPR)
E4	CORE	Perform Radio Direction Findings (RDF) of Signals of Interest (SOI)
E5	CORE	Perform waveform analysis
E5	CORE	Perform wavelength to frequency conversions

EQUIPMENT MAINTENANCE

Paygrade	**Task Type**	**Task Statements**
E4	CORE	Analyze network audit logs
E5	NON-CORE	Implement Emissions Control (EMCON)
E4	CORE	Review equipment status for proper operation

NETWORK MANAGEMENT

Paygrade	**Task Type**	**Task Statements**
E4	CORE	Apply Information Systems (IS) file and folder permissions

NETWORK OPERATIONS

Paygrade	**Task Type**	**Task Statements**
E4	CORE	Administer computer Information System (IS) user accounts
E4	CORE	Analyze Information System (IS) trends (e.g., hardware, software, network, etc.)
E5	CORE	Verify delivered Information Systems (IS) functionality (i.e., System Operational Verification Test (SOVT))
E5	CORE	Verify delivered network components functionality (i.e., System Operational Verification Test (SOVT))
E5	CORE	Verify delivered system hardware functionality (i.e., System Operational Verification Test (SOVT))