

CHAPTER 20



CRYPTOLOGIC TECHNICIAN (COLLECTIONS) (CTR)

NAVPERS 18068F-20M
Change 91

Updated: July 2022

Enclosure (1)

TABLE OF CONTENTS
CRYPTOLOGIC TECHNICIAN (COLLECTIONS) (CTR)

SCOPE OF RATING	CTR-4
GENERAL INFORMATION	CTR-5
ANALYST AND REPORTER	CTR-6
FIREPOWER EMPLOYMENT	CTR-6
FORCE PROTECTION	CTR-7
INFORMATION OPERATION SUPPORT	CTR-7
INTELLIGENCE ANALYSIS AND PRODUCTION	CTR-7
INTELLIGENCE AND DATA COLLECTION	CTR-9
INTELLIGENCE INTEGRATION AND DISSEMINATION	CTR-9
INTELLIGENCE PLANNING AND DIRECTION	CTR-10
INTELLIGENCE PROCESSING AND EXPLOITATION	CTR-12
NETWORK EXPLOITATION	CTR-12
TRAINING	CTR-12
SIGNALS ANALYST	CTR-13
FIREPOWER EMPLOYMENT	CTR-13
FORCE PROTECTION	CTR-13
INFORMATION OPERATION SUPPORT	CTR-14
INTELLIGENCE ANALYSIS AND PRODUCTION	CTR-14
INTELLIGENCE AND DATA COLLECTION	CTR-15
INTELLIGENCE INTEGRATION AND DISSEMINATION	CTR-15
INTELLIGENCE PLANNING AND DIRECTION	CTR-15
INTELLIGENCE PROCESSING AND EXPLOITATION	CTR-16
NETWORK EXPLOITATION	CTR-17
TRAINING	CTR-17
COLLECTION OPERATOR	CTR-18
FIREPOWER EMPLOYMENT	CTR-18
FORCE PROTECTION	CTR-19
INFORMATION OPERATION SUPPORT	CTR-19
INTELLIGENCE ANALYSIS AND PRODUCTION	CTR-19
INTELLIGENCE AND DATA COLLECTION	CTR-20
INTELLIGENCE INTEGRATION AND DISSEMINATION	CTR-22
INTELLIGENCE PLANNING AND DIRECTION	CTR-22
INTELLIGENCE PROCESSING AND EXPLOITATION	CTR-23
NETWORK EXPLOITATION	CTR-24
TRAINING	CTR-24

TABLE OF CONTENTS (CONT'D)
CRYPTOLOGIC TECHNICIAN (COLLECTIONS) (CTR)

CYBER ANALYST AND REPORTER	CTR-25
FIREPOWER EMPLOYMENT	CTR-25
FORCE PROTECTION	CTR-25
INFORMATION OPERATION SUPPORT	CTR-26
INTELLIGENCE ANALYSIS AND PRODUCTION	CTR-26
INTELLIGENCE AND DATA COLLECTION	CTR-27
INTELLIGENCE INTEGRATION AND DISSEMINATION	CTR-28
INTELLIGENCE PLANNING AND DIRECTION	CTR-28
INTELLIGENCE PROCESSING AND EXPLOITATION	CTR-30
NETWORK EXPLOITATION	CTR-30
TRAINING	CTR-31

NAVY ENLISTED OCCUPATIONAL STANDARD
FOR
CRYPTOLOGIC TECHNICIAN (COLLECTION) (CTR)



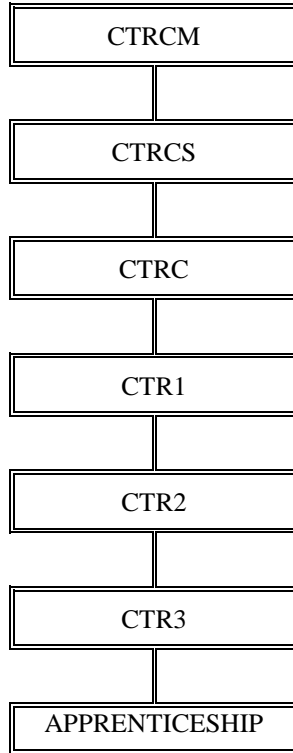
SCOPE OF RATING

Cryptologic Technicians (Collection) (CTR) operate advanced computer systems to conduct Information and Cyberspace Operations; collect, analyze, and exploit Signals Of Interest (SOI) throughout the Radio Frequency (RF) spectrum to identify, locate, and report worldwide threats; control, inventory, and safeguard access to classified material and information systems; provide tactical, digital network, strategic signals intelligence, technical guidance, targeting solutions, and Signals Intelligence (SIGINT) support to surface, subsurface, air, space, special operations forces, and National consumers to maintain information superiority.

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 18068M) as Chapter 20.

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**Analyst And Reporter****Job Code****001072****Job Family**

Protective Service

NOC

TBD

Short Title (30 Characters)

ANALYST AND REPORTER

Short Title (14 Characters)

ANLYST&REPORTR

Pay Plan

Enlisted

Career Field

CTR

Other Relationships and Rules

NECs CXXX series and other NECs as assigned

Job Description

Analysts and Reporters develop targets in support of Information Operations (IO); collect, analyze, and fuse target communications and multiple source information identifying Essential Elements of Information (EIs) to map and develop target networks, conduct spatial and temporal geolocation analysis, and execute geolocation operations and data extractions; access and manipulate databases to perform planning and fusion analysis; develop targets for communications Electronic Attack (EA) and cyberspace planning, execution, and assessment; provide Area of Responsibility (AOR) specific Signals Intelligence (SIGINT) trend and predictive analysis in support of Priority Intelligence Requirements (PIRs); draft and disseminate Signals Intelligence (SIGINT) reports, cryptologic mission reports, cryptologic and all-source assessments, sanitized product reports, and emergency action plans; conduct analysis in support of Cyberspace Operations to meet National, Fleet, and Joint requirements; control and safeguard classified information to include storage, transportation, and protection.

DoD Relationship**Group Title**Intercept Operators
(Code and Non-Code)**DoD Code**

123100

O*NET Relationship**Occupation Title**

Protective Service

SOC Code

33-3021.00

Job Family

Protective Service

Skills*Critical Thinking**Reading Comprehension**Judgment and Decision Making**Complex Problem Solving**Management of Material Resources**Coordination**Science**Systems Analysis**Mathematics**Writing***Abilities***Deductive Reasoning**Inductive Reasoning**Written Comprehension**Written Expression**Speed of Closure**Information Ordering**Category Flexibility**Oral Expression**Problem Sensitivity**Selective Attention***FIREPOWER EMPLOYMENT****Paygrade****Task Type****Task Statements**

E5

NON-CORE

Assess Measures of Performance (MOP)

E5

NON-CORE

Brief post-communication Electronic Attack (EA) assessments

E4

CORE

Comply with current communications Electronic Warfare (EW) Rules of Engagement (ROE)

E5

NON-CORE

Conduct Battle Damage Assessments (BDA)

E5

NON-CORE

Conduct Counter-Unmanned Aerial Systems (C-UAS) operations

E7

NON-CORE

Develop communication Electronic Attack (EA) plans

E7

NON-CORE

Develop communications Electronic Attack (EA) Concept of Operations (CONOP)

E6

NON-CORE

Evaluate Measures of Effectiveness (MOE)

FORCE PROTECTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Analyze unmanned vehicles communications for targeting
E4	CORE	Control access to restricted areas
E4	CORE	Destroy Sensitive Compartmented Information (SCI) materials
E4	CORE	Document receipt of classified materials
E7	CORE	Enforce Operations Security (OPSEC)
E5	NON-CORE	Evaluate threat envelopes
E4	CORE	Implement Emergency Action Plans (EAP)
E7	NON-CORE	Manage Sensitive Compartmented Information Facility (SCIF) accreditations
E4	CORE	Properly mark Sensitive Compartmented Information (SCI) materials
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Transport Sensitive Compartmented Information (SCI) materials

INFORMATION OPERATION SUPPORT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Conduct Military Information Support Operations (MISO)
E7	CORE	Coordinate Information Related Capabilities (IRC)
E4	CORE	Provide Military Deception (MILDEC) support

INTELLIGENCE ANALYSIS AND PRODUCTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Analyze collection sources
E5	NON-CORE	Analyze Command and Control Warfare (C2W) networks for critical nodes
E5	NON-CORE	Analyze Command, Control, Communications, Computers, Cyberspace, Intelligence, Surveillance, Reconnaissance, and Target (C5ISR) networks for critical nodes
E4	NON-CORE	Analyze common Satellite Communications (SATCOM) related elements
E4	NON-CORE	Analyze communication device capabilities
E4	CORE	Analyze Communication External (COMEXT) target usage
E5	CORE	Analyze Foreign Instrumentation Signals Intelligence (FISINT) to meet mission requirements
E4	CORE	Analyze intercept to identify Essential Elements of Information (EEI)
E5	NON-CORE	Analyze network intrusion global threat activity data
E5	CORE	Analyze PROFORMA to meet mission requirements
E4	NON-CORE	Analyze Ultra High Frequency/Very High Frequency/Push To Talk (UHF/VHF/PTT) communications for exploitation
E4	CORE	Analyze unmanned vehicles communications for exploitation
E5	NON-CORE	Conduct Network Oriented Data Acquisition Language (NODAL) analysis
E4	NON-CORE	Determine intelligence document source
E5	CORE	Develop Area of Responsibility (AOR) target data
E5	NON-CORE	Develop pattern of life analysis
E5	CORE	Develop target packages
E5	CORE	Develop target profiles

INTELLIGENCE ANALYSIS AND PRODUCTION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	CORE	Develop targets in support of commander's intent
E4	NON-CORE	Draft fused Signals Intelligence (SIGINT) reports
E4	NON-CORE	Draft intelligence product reports
E5	CORE	Draft post-mission reports
E4	CORE	Draft time sensitive reports
E5	NON-CORE	Edit serialized intelligence reports for dissemination
E6	NON-CORE	Evaluate adversary critical capabilities, requirements, and vulnerabilities
E4	NON-CORE	Fuse technical data to develop target communications profiles
E5	NON-CORE	Identify adversary critical capabilities, requirements, and vulnerabilities
E5	CORE	Identify adversary Tactics, Techniques, and Procedures (TTP)
E5	CORE	Map communications networks
E5	NON-CORE	Perform advanced characterization of the electronic environment
E4	NON-CORE	Perform all-source analysis
E5	NON-CORE	Perform asset source validation
E4	CORE	Perform content analysis
E4	CORE	Perform geolocation analysis
E4	CORE	Perform metadata analysis
E5	NON-CORE	Perform non-traditional targeting operations
E5	NON-CORE	Perform Sensitive Site Exploitation (SSE) analysis
E5	CORE	Perform Signals Intelligence (SIGINT) fusion analysis
E4	NON-CORE	Perform Signals Intelligence (SIGINT) Geospatial Analysis (SGA)
E4	CORE	Perform Signals Intelligence (SIGINT) research using Intelligence Community (IC) databases to meet mission requirements
E5	NON-CORE	Perform technical target analysis
E4	CORE	Perform traffic analysis
E5	NON-CORE	Perform Unattended Ground Sensor (UGS) analysis
E5	NON-CORE	Perform untethered analysis
E5	CORE	Produce target communications profiles using technical data
E5	NON-CORE	Provide Signals Intelligence (SIGINT) support to targetteering
E5	NON-CORE	Provide target Positive Identification (PID)
E6	NON-CORE	Release serialized intelligence reports for dissemination
E5	CORE	Research network technologies
E4	CORE	Research Open Source Intelligence (OSINT)
E4	CORE	Respond to Request For Information (RFI)
E5	CORE	Review time sensitive reports
E6	CORE	Validate SIGINT product reports
E6	NON-CORE	Validate technical aspects of cyberspace operations products

INTELLIGENCE AND DATA COLLECTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Align Cyberspace tasking to mission requirements
E4	NON-CORE	Analyze Electromagnetic (EM) spectrum for targeting
E4	CORE	Assess Indication & Warning (I&W) threats
E4	CORE	Assign identifiers to target platforms
E6	NON-CORE	Develop automation processes
E4	CORE	Execute commands within various Operating Systems (OS)
E4	CORE	Generate Request For Information (RFI)
E4	NON-CORE	Identify traffic source for targeting
E4	CORE	Maintain target lists (e.g., Regional Target List (RTL), Joint Target List (JTL), Combined Target List (CTL))
E7	NON-CORE	Manage Command Readiness Training Team (CRTT)
E6	CORE	Manage geolocation operations
E4	CORE	Perform geolocation of Signals of Interest (SOI)
E5	NON-CORE	Perform Radio Frequency (RF) propagation modeling
E5	CORE	Provide feedback to developers on signals collection, processing, and analysis tools to mitigate existing shortfalls
E4	CORE	Review equipment status
E4	CORE	Troubleshoot system equipment failures and errors
E4	CORE	Troubleshoot system software failures and errors
E5	CORE	Validate mission plans
E5	CORE	Verify collected information meets intelligence needs

INTELLIGENCE INTEGRATION AND DISSEMINATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Brief intelligence operations
E4	CORE	Brief Signal Intelligence (SIGINT) Operations and capabilities
E5	CORE	Coordinate target analysis with external units
E4	CORE	Disseminate time sensitive reports
E6	CORE	Evaluate analysis and reporting operations
E7	CORE	Manage dissemination of Signals Intelligence (SIGINT) reports
E4	CORE	Provide Indications and Warnings (I&W) to tactical commanders
E5	CORE	Provide Time Sensitive Target (TST) operations intelligence support
E5	CORE	Sanitize cryptologic data for dissemination

INTELLIGENCE PLANNING AND DIRECTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	CORE	Analyze collection metrics
E7	CORE	Assign assets and resources to meet intelligence requirements
E5	NON-CORE	Collaborate with Intelligence Community (IC) analysts for cyberspace operations
E5	CORE	Compile collection metrics
E4	CORE	Comply with Intelligence Oversight (IO) requirements
E5	NON-CORE	Conduct Intelligence Preparation of the Operating Environment (IPOE)
E5	NON-CORE	Conduct Joint Intelligence Preparation of the Operational Environment (JIPOE)
E7	NON-CORE	Construct collection matrix
E7	CORE	Construct collection plans
E6	CORE	Coordinate available intelligence resources
E7	CORE	Coordinate Concept of Operations (CONOPS) through Battleforce Stakeholders
E7	NON-CORE	Coordinate cyberspace operations with Special Access Program (SAP)/Integrated Joint Special Technical Operations (IJSTO) planners/Review and Approval Process for Cyber Operations (RAPCO)
E5	CORE	Coordinate geolocation operations
E7	CORE	Coordinate mission operations
E7	CORE	Coordinate Signals Intelligence (SIGINT) Indications and Warnings (I&W)
E5	NON-CORE	Coordinate target vetting with appropriate partners
E7	CORE	Create cryptologic tasking for mission requirements
E7	CORE	Cross-check Intelligence Requirements (IR)
E5	NON-CORE	Deconflict frequency usage
E5	NON-CORE	Deconflict network operations
E5	CORE	Determine collection gaps
E6	CORE	Determine collection requirements
E7	CORE	Determine intelligence gaps
E5	NON-CORE	Develop communications Electronic Attack (EA) briefs
E6	NON-CORE	Develop Offensive Cyberspace Operations (OCO) Operations Plans (OPLAN)
E5	NON-CORE	Develop target templates
E7	CORE	Direct Signals Intelligence (SIGINT) taskings
E7	CORE	Draft Signals Intelligence (SIGINT) operations policies and procedures
E6	CORE	Enforce compliance with Intelligence Oversight (IO) requirements
E5	NON-CORE	Establish communications infrastructure for data exfiltration
E7	CORE	Evaluate collection metrics
E4	CORE	Identify information flow within the intelligence cycle (Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED))
E4	CORE	Implement United States Signals Intelligence Directives (USSID)

INTELLIGENCE PLANNING AND DIRECTION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Incorporate Commanders Critical Information Requirements (CCIRs) to include priority intelligence requirements (PIR) into collection management activities
E7	CORE	Incorporate National Intelligence Priorities Framework (NIPF)
E6	NON-CORE	Integrate cyberspace targeting efforts with other organization and combatant commands
E6	NON-CORE	Manage accesses on a Mission Correlation Table (MCT)
E7	CORE	Manage Critical (CRITIC) message programs
E6	NON-CORE	Manage cyberspace taskings
E7	CORE	Manage Information Related Capability (IRC) programs
E7	CORE	Manage intelligence support solutions
E6	NON-CORE	Manage Radio Frequency (RF) propagation modeling
E7	CORE	Manage Signals Intelligence (SIGINT) and cyber mission requirement resources
E7	CORE	Manage targeting cycles
E5	NON-CORE	Perform database auditing
E6	NON-CORE	Perform predictive analysis of adversary actions in cyberspace
E7	CORE	Prioritize Intelligence Requirements (IR)
E4	CORE	Produce area of interest briefs
E5	NON-CORE	Provide aim point recommendations
E6	NON-CORE	Provide coordination, validation, and management assistance of intelligence collection requirements, plans, and/or activities
E6	CORE	Provide coordination, validation, and management assistance of Signals Intelligence (SIGINT) collection requirements, plans, and/or activities
E5	CORE	Provide target nomination recommendations which meet commander's objectives
E4	CORE	Research military Order of Battle (OOB)
E4	CORE	Research Signals Intelligence (SIGINT) Order of Battle (OOB)
E7	CORE	Submit Cryptologic capabilities requirements for implementation and mission sustainment
E6	CORE	Submit priority recommendations to support Commander's Critical Information Requirements (CCIR)
E5	CORE	Supervise Intelligence, Surveillance, and Reconnaissance (ISR) operations
E7	CORE	Validate Collection Management Authority (CMA) requirements in support of Intelligence, Surveillance and Reconnaissance (ISR) Concept of Operations (CONOPS)
E5	CORE	Verify mission taskings

INTELLIGENCE PROCESSING AND EXPLOITATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Analyze multiple access schemes
E4	NON-CORE	Analyze wireless communications for targeting
E5	NON-CORE	Assess collateral effects of targeting operations
E6	NON-CORE	Construct tools for analysis
E4	CORE	Convert numbering systems
E4	CORE	Correlate case notations
E4	CORE	Determine Communication Emitter Notations (CENOT)
E5	NON-CORE	Develop scripts and programs
E5	NON-CORE	Perform Counter-Unmanned Aerial Systems (C-UAS) analysis
E4	CORE	Perform File Transfer Protocol (FTP)
E4	CORE	Perform target exploitation operations
E4	NON-CORE	Perform track management and target identification

NETWORK EXPLOITATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	NON-CORE	Analyze digital network communications
E5	NON-CORE	Analyze network device configurations
E5	NON-CORE	Analyze network security architecture components
E5	NON-CORE	Analyze network traffic to identify anomalous activity and potential threats
E5	NON-CORE	Conduct mid-point analysis (e.g., routers, firewalls, etc.)
E5	NON-CORE	Determine basic structure and architecture of networks
E5	NON-CORE	Determine Operating System (OS) characteristics
E5	NON-CORE	Determine software and hardware vulnerabilities
E6	NON-CORE	Evaluate information networks defensive posture of target networks
E5	NON-CORE	Map digital networks
E5	NON-CORE	Perform file system analysis
E5	NON-CORE	Perform packet capture (PCAP) analysis
E4	NON-CORE	Perform protocol analysis

TRAINING

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Conduct operational certifications
E5	NON-CORE	Implement Command Readiness Training Team (CRTT)
E5	CORE	Maintain awareness of advancements in hardware and software technologies and their potential vulnerabilities

Job Title
Signals Analyst

Job Code
001077

Job Family
 Computer and Mathematical

NOC
 TBD

Short Title (30 Characters)
 SIGNALS ANALYST

Short Title (14 Characters)
 SIGNALS ANALYST

Pay Plan
 Enlisted

Career Field
 CTR

Other Relationships and Rules
 NECs CXXX series and other NECs as assigned

Job Description

Signals Analysts conduct signals search, analysis, target identification, and reporting operations; develop, evaluate, and execute target mission plans to include exploitation, manipulation, and management of the Electromagnetic (EM) spectrum; collect and process Signals of Interest (SOI) employing demodulation, demultiplexing techniques, and coding theory; perform in-depth analysis of waveform propagation, theory and reporting of known, new, and anomalous signals, and provide locational data; research and develop signals; perform digital communications and bit stream analysis to recover signals structures and utilize internal parameters to identify Signals Of Interest (SOI); construct waveforms in support of communication electronic attack and integrated fires; conduct protocol analysis; develop scripts and tools for Cyberspace Operations to meet National, Fleet, and Joint requirements; control and safeguard classified information to include storage, transportation, and protection.

DoD Relationship

Group Title
 Intercept Operators
 (Code and Non-Code)

DoD Code
 123100

O*NET Relationship

Occupation Title
 Computer Programmers

SOC Code
 15-1251.00

Job Family
 Computer and Mathematical

Skills

Science
Mathematics
Reading Comprehension
Critical Thinking
Judgment and Decision Making
Complex Problem Solving
Operation and Control
Management of Material Resources
Systems Analysis
Writing

Abilities

Deductive Reasoning
Inductive Reasoning
Information Ordering
Written Comprehension
Written Expression
Speed of Closure
Flexibility of Closure
Category Flexibility
Problem Sensitivity
Mathematical Reasoning

FIREPOWER EMPLOYMENT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Create Electronic Attack (EA) waveforms

FORCE PROTECTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Control access to restricted areas
E4	CORE	Destroy Sensitive Compartmented Information (SCI) materials
E4	CORE	Document receipt of classified materials
E7	CORE	Enforce Operations Security (OPSEC)
E4	CORE	Implement Emergency Action Plans (EAP)
E7	NON-CORE	Manage Sensitive Compartmented Information Facility (SCIF) accreditations
E5	NON-CORE	Perform electronic counter-surveillance
E4	CORE	Properly mark Sensitive Compartmented Information (SCI) materials
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Transport Sensitive Compartmented Information (SCI) materials

INFORMATION OPERATION SUPPORT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Conduct Military Information Support Operations (MISO)
E4	CORE	Provide Military Deception (MILDEC) support

INTELLIGENCE ANALYSIS AND PRODUCTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Analyze collection sources
E4	NON-CORE	Analyze common Satellite Communications (SATCOM) related elements
E4	NON-CORE	Analyze communication device capabilities
E5	CORE	Analyze Foreign Instrumentation Signals Intelligence (FISINT) to meet mission requirements
E4	CORE	Analyze intercept to identify Essential Elements of Information (EEI)
E5	NON-CORE	Analyze network vulnerabilities
E4	CORE	Analyze non-communications signals
E5	CORE	Analyze PROFORMA to meet mission requirements
E4	CORE	Analyze short duration signals
E5	NON-CORE	Analyze signal internal overhead
E5	NON-CORE	Analyze spread spectrum Signals of Interest (SOI)
E4	NON-CORE	Analyze Ultra High Frequency/Very High Frequency/Push To Talk (UHF/VHF/PTT) communications for exploitation
E5	CORE	Develop Area of Responsibility (AOR) target data
E4	NON-CORE	Develop Communication External (COMEXT) notations
E5	CORE	Draft post-mission reports
E4	NON-CORE	Draft signals analysis reports
E6	NON-CORE	Perform advanced bit stream analysis
E5	NON-CORE	Perform advanced characterization of the electronic environment
E4	CORE	Perform content analysis
E4	CORE	Perform geolocation analysis
E5	NON-CORE	Perform intermediate bit stream analysis
E4	CORE	Perform metadata analysis
E4	CORE	Perform Signals Intelligence (SIGINT) research using Intelligence Community (IC) databases to meet mission requirements
E5	NON-CORE	Perform technical target analysis
E5	CORE	Produce target communications profiles using technical data
E5	CORE	Research network technologies
E4	CORE	Research Open Source Intelligence (OSINT)
E4	CORE	Respond to Request For Information (RFI)
E5	CORE	Review time sensitive reports

INTELLIGENCE AND DATA COLLECTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Analyze Electromagnetic (EM) spectrum for exploitation
E4	CORE	Assign identifiers to target platforms
E5	NON-CORE	Create Signal Descriptor Files (SDF)
E4	CORE	Demodulate Signals of Interest (SOI)
E6	NON-CORE	Develop automation processes
E4	CORE	Execute commands within various Operating Systems (OS)
E5	NON-CORE	Exploit modulation types
E4	CORE	Generate Request For Information (RFI)
E4	CORE	Identify Signals of Interest (SOI)
E7	NON-CORE	Manage Command Readiness Training Team (CRTT)
E4	CORE	Modify Signal Descriptor Files (SDF)
E5	CORE	Optimize collection systems
E4	CORE	Perform Target Research Technical Development (TRTD) operations
E5	CORE	Provide feedback to developers on signals collection, processing, and analysis tools to mitigate existing shortfalls
E4	CORE	Review equipment status
E4	CORE	Troubleshoot system equipment failures and errors
E4	CORE	Troubleshoot system software failures and errors
E5	CORE	Validate mission plans
E5	NON-CORE	Validate Signal Descriptor Files (SDF)
E4	CORE	Validate system Radio Frequency (RF) distribution paths
E5	CORE	Verify collected information meets intelligence needs
E5	NON-CORE	Verify Signal Descriptor Files (SDF) performance

INTELLIGENCE INTEGRATION AND DISSEMINATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Brief intelligence operations
E4	CORE	Brief Signal Intelligence (SIGINT) Operations and capabilities
E5	CORE	Sanitize cryptologic data for dissemination

INTELLIGENCE PLANNING AND DIRECTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	CORE	Analyze collection metrics
E7	CORE	Assign assets and resources to meet intelligence requirements
E5	CORE	Compile collection metrics
E4	CORE	Comply with Intelligence Oversight (IO) requirements
E7	CORE	Coordinate mission operations
E7	CORE	Create cryptologic tasking for mission requirements
E7	CORE	Cross-check Intelligence Requirements (IR)
E7	CORE	Draft Signals Intelligence (SIGINT) operations policies and procedures

INTELLIGENCE PLANNING AND DIRECTION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	CORE	Enforce compliance with Intelligence Oversight (IO) requirements
E7	CORE	Evaluate collection metrics
E4	CORE	Identify information flow within the intelligence cycle (Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED))
E4	CORE	Implement United States Signals Intelligence Directives (USSID)
E7	CORE	Incorporate Commanders Critical Information Requirements (CCIRs) to include priority intelligence requirements (PIR) into collection management activities
E6	NON-CORE	Manage accesses on a Mission Correlation Table (MCT)
E7	CORE	Manage Critical (CRITIC) message programs
E7	CORE	Manage Information Related Capability (IRC) programs
E7	CORE	Manage intelligence support solutions
E5	NON-CORE	Perform database auditing
E7	CORE	Prioritize Intelligence Requirements (IR)
E6	CORE	Provide coordination, validation, and management assistance of Signals Intelligence (SIGINT) collection requirements, plans, and/or activities
E5	CORE	Provide target nomination recommendations which meet commander's objectives
E7	CORE	Submit Cryptologic capabilities requirements for implementation and mission sustainment
E6	CORE	Submit priority recommendations to support Commander's Critical Information Requirements (CCIR)

INTELLIGENCE PROCESSING AND EXPLOITATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Analyze digital speech
E4	CORE	Analyze modems
E4	CORE	Analyze multiple access schemes
E5	NON-CORE	Analyze pulse code formats
E4	CORE	Analyze wireless communications for exploitation
E6	NON-CORE	Construct tools for analysis
E4	CORE	Convert numbering systems
E4	CORE	Correlate case notations
E4	CORE	Demodulate basic signals
E5	NON-CORE	Demultiplex intermediate signals
E5	NON-CORE	Demultiplex known signals
E6	NON-CORE	Demultiplex unknown signals
E4	CORE	Detect bit synchronizers
E5	NON-CORE	Detect signal anomalies from signals analysis
E4	CORE	Determine Communication Emitter Notations (CENOT)
E4	NON-CORE	Determine digital line coding schemes
E4	CORE	Determine error detection and correction schemes

INTELLIGENCE PROCESSING AND EXPLOITATION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Determine Linear Recursive Sequences (LRS)
E4	CORE	Determine short duration and non-communications signals
E5	NON-CORE	Develop scripts and programs
E4	CORE	Forward digitized signals
E4	NON-CORE	Identify Communication External Notations (COMEXT)
E4	CORE	Identify Foreign Instrumentation Signals Intelligence (FISINT) to meet mission requirements
E4	CORE	Identify PROFORMA to meet mission requirements
E6	NON-CORE	Perform advanced demodulations
E4	CORE	Perform basic bit stream analysis
E4	CORE	Perform File Transfer Protocol (FTP)
E4	CORE	Perform target exploitation operations
E4	CORE	Perform waveform analysis
E4	CORE	Perform wavelength to frequency conversions
E4	CORE	Process Signals of Interest (SOI)
E4	CORE	Verify internal signal structures

NETWORK EXPLOITATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	NON-CORE	Analyze digital network communications
E5	NON-CORE	Analyze known and non-standard protocols
E6	NON-CORE	Analyze unidentified protocols
E5	NON-CORE	Conduct proximal access network operations
E5	NON-CORE	Detect network vulnerabilities
E5	NON-CORE	Determine basic structure and architecture of networks
E4	NON-CORE	Perform protocol analysis
E4	CORE	Process digital network communications

TRAINING

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Conduct operational certifications
E5	NON-CORE	Implement Command Readiness Training Team (CRTT)
E5	CORE	Maintain awareness of advancements in hardware and software technologies and their potential vulnerabilities

Job Title**Collection Operator****Job Code****002746****Job Family**

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

COLLECTION OPERATOR

Short Title (14 Characters)

COLL OPERATOR

Pay Plan

Enlisted

Career Field

CTR

Other Relationships and Rules

NECs CXXX series and other NECs as assigned

Job Description

Collection Operators operate and manage collection systems to intercept and analyze Signals of Interest (SOI) for the purpose of identification, exploitation, and reporting in support of community National, Joint, and Fleet, intelligence requirements; identify, track, and report adversary geographic locations to support target identification and military operations; perform information operations to deceive, degrade, or deny adversaries' electronic sensors; perform own force monitoring to prevent adversary from utilizing friendly force emissions; optimize Signals Intelligence (SIGINT) collection resources and prioritize tasking; develop relationships between mission requirements, resource management, operating procedures, and communications target procedural identification techniques; manage signals collection, Request for Information (RFI), analysis, reporting, special intelligence communication networks, and assigned personnel; develop and execute courses of action in response to consumer feedback; and comply with emergency action plans, sanitization and release authorities, classified information storage, transportation, and protection requirements.

DoD Relationship*Group Title*Intercept Operators
(Code and Non-Code)*DoD Code*

123100

O*NET Relationship*Occupation Title*

Information Security Analysts

SOC Code

15-1212.00

Job Family

Computer and Mathematical

Skills*Operation and Control**Reading Comprehension**Critical Thinking**Management of Material Resources**Coordination**Equipment Selection**Judgment and Decision Making**Science**Complex Problem Solving**Mathematics***Abilities***Deductive Reasoning**Inductive Reasoning**Written Comprehension**Information Ordering**Speed of Closure**Written Expression**Category Flexibility**Problem Sensitivity**Oral Expression**Spatial Orientation***FIREPOWER EMPLOYMENT****Paygrade**

E5

Task Type

NON-CORE

Task Statements

Assess Measures of Performance (MOP)

E5

NON-CORE

Brief post-communication Electronic Attack (EA) assessments

E4

CORE

Collect Battle Damage Indicators (BDI)

E4

CORE

Comply with current communications Electronic Warfare (EW) Rules of Engagement (ROE)

E5

NON-CORE

Conduct Counter-Unmanned Aerial Systems (C-UAS) operations

E5

CORE

Conduct Electronic Attack (EA) missions

E5

NON-CORE

Create Electronic Attack (EA) waveforms

E7

NON-CORE

Develop communication Electronic Attack (EA) plans

E7

NON-CORE

Develop communications Electronic Attack (EA) Concept of Operations (CONOP)

E6

NON-CORE

Evaluate Measures of Effectiveness (MOE)

FORCE PROTECTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Analyze unmanned vehicles communications for targeting
E4	CORE	Control access to restricted areas
E4	CORE	Destroy Sensitive Compartmented Information (SCI) materials
E4	CORE	Document receipt of classified materials
E7	CORE	Enforce Operations Security (OPSEC)
E4	CORE	Implement Emergency Action Plans (EAP)
E6	CORE	Manage Communication Security (COMSEC) monitoring
E6	CORE	Manage Own Force Monitoring (OFM)
E7	NON-CORE	Manage Sensitive Compartmented Information Facility (SCIF) accreditations
E4	CORE	Perform Communication Security (COMSEC) monitoring
E4	CORE	Perform Counter-Intelligence, Surveillance, and Reconnaissance (C-ISR)
E5	NON-CORE	Perform electronic counter-surveillance
E4	CORE	Properly mark Sensitive Compartmented Information (SCI) materials
E4	CORE	Report Electronic Attack (EA) against friendly units, systems, links or nodes
E4	CORE	Safeguard Sensitive Compartmented Information (SCI) materials
E4	CORE	Transport Sensitive Compartmented Information (SCI) materials

INFORMATION OPERATION SUPPORT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Perform Electronic Warfare (EW) support
E5	NON-CORE	Conduct Military Information Support Operations (MISO)
E7	CORE	Coordinate Information Related Capabilities (IRC)
E4	CORE	Perform Own Force Monitoring (OFM)
E4	CORE	Provide Military Deception (MILDEC) support

INTELLIGENCE ANALYSIS AND PRODUCTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Analyze collection sources
E4	NON-CORE	Analyze communication device capabilities
E4	CORE	Analyze Communication External (COMEXT) target usage
E4	CORE	Analyze intercept to identify Essential Elements of Information (EEI)
E4	CORE	Analyze unmanned vehicles communications for exploitation
E5	CORE	Develop Area of Responsibility (AOR) target data
E5	NON-CORE	Develop pattern of life analysis
E5	CORE	Draft post-mission reports
E4	CORE	Draft time sensitive reports
E6	NON-CORE	Evaluate adversary critical capabilities, requirements, and vulnerabilities
E5	NON-CORE	Identify adversary critical capabilities, requirements, and vulnerabilities
E5	CORE	Identify adversary Tactics, Techniques, and Procedures (TTP)

INTELLIGENCE ANALYSIS AND PRODUCTION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Perform advanced characterization of the electronic environment
E4	CORE	Perform content analysis
E4	CORE	Perform geolocation analysis
E4	CORE	Perform metadata analysis
E4	CORE	Perform Signals Intelligence (SIGINT) research using Intelligence Community (IC) databases to meet mission requirements
E5	NON-CORE	Perform technical target analysis
E4	CORE	Perform traffic analysis
E5	NON-CORE	Perform untethered analysis
E4	CORE	Research Open Source Intelligence (OSINT)
E4	CORE	Respond to Request For Information (RFI)
E5	CORE	Review time sensitive reports
E6	CORE	Validate SIGINT product reports

INTELLIGENCE AND DATA COLLECTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Align Cyberspace tasking to mission requirements
E4	CORE	Allocate Signals Intelligence (SIGINT) collection resources to assigned tasking
E4	CORE	Analyze Electromagnetic (EM) spectrum for exploitation
E4	CORE	Assess Indication & Warning (I&W) threats
E4	CORE	Collect Signals Of Interest (SOI)
E5	NON-CORE	Conduct low visibility collection operations/unconventional collections
E4	CORE	Conduct wireless surveys
E4	CORE	Configure systems for signals collection
E4	CORE	Create mission plans
E4	CORE	Demodulate Signals of Interest (SOI)
E6	NON-CORE	Develop automation processes
E5	NON-CORE	Establish command and control link for Unmanned Aerial Systems (UAS) payloads
E4	CORE	Execute commands within various Operating Systems (OS)
E5	NON-CORE	Exploit modulation types
E5	NON-CORE	Fabricate collection equipment (Commercial Off The Shelf/Government Off The Shelf (COTS/GOTS))
E4	CORE	Generate Request For Information (RFI)
E4	CORE	Identify Signals of Interest (SOI)
E4	CORE	Implement cryptologic taskings
E4	CORE	Maintain position logs
E4	CORE	Maintain target lists (e.g., Regional Target List (RTL), Joint Target List (JTL), Combined Target List (CTL))
E6	CORE	Manage collection of Signals of Interest (SOI)

INTELLIGENCE AND DATA COLLECTION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	CORE	Manage collection system operations and configurations
E7	NON-CORE	Manage Command Readiness Training Team (CRTT)
E7	CORE	Manage exploitation of Electromagnetic (EM) spectrum
E6	CORE	Manage geolocation operations
E4	CORE	Modify Signal Descriptor Files (SDF)
E4	CORE	Monitor Signals of Interest (SOI) frequencies
E5	CORE	Optimize collection systems
E4	CORE	Perform geolocation of Signals of Interest (SOI)
E4	CORE	Perform geolocation/Direction Finding (DF) of distress signals
E5	NON-CORE	Perform ground terminal guidance operations
E4	NON-CORE	Perform morse code operations
E4	CORE	Perform Radio Direction Findings (RDF) of Signals of Interest (SOI)
E5	NON-CORE	Perform Radio Frequency (RF) propagation modeling
E4	CORE	Perform remote access operations
E5	NON-CORE	Perform Sensitive Site Exploitation (SSE) operations
E5	NON-CORE	Perform tactical collection operations
E5	NON-CORE	Perform tactical Signals Intelligence (SIGINT) Intelligence, Surveillance, and Reconnaissance (ISR)
E5	NON-CORE	Perform tactical survey operations
E4	CORE	Perform Target Research Technical Development (TRTD) operations
E5	NON-CORE	Perform Unattended Ground Sensor (UGS) emplacement operations
E5	NON-CORE	Perform untethered collections
E5	CORE	Provide feedback to developers on signals collection, processing, and analysis tools to mitigate existing shortfalls
E4	CORE	Record signals for post collection analysis
E4	CORE	Review equipment status
E4	CORE	Select antennas for signals exploitation
E4	CORE	Select receivers for signals exploitation
E4	CORE	Shutdown collection systems
E4	CORE	Start-up collection systems
E6	CORE	Supervise collection operations
E4	CORE	Troubleshoot system equipment failures and errors
E4	CORE	Troubleshoot system software failures and errors
E5	CORE	Validate mission plans
E4	CORE	Validate system Radio Frequency (RF) distribution paths
E5	CORE	Verify collected information meets intelligence needs
E5	NON-CORE	Verify Signal Descriptor Files (SDF) performance

INTELLIGENCE INTEGRATION AND DISSEMINATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Brief intelligence operations
E4	CORE	Brief Signal Intelligence (SIGINT) Operations and capabilities
E4	CORE	Disseminate time sensitive reports
E7	CORE	Manage dissemination of Signals Intelligence (SIGINT) reports
E4	CORE	Provide Indications and Warnings (I&W) to tactical commanders
E5	CORE	Provide Time Sensitive Target (TST) operations intelligence support
E5	CORE	Sanitize cryptologic data for dissemination

INTELLIGENCE PLANNING AND DIRECTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	CORE	Analyze collection metrics
E7	CORE	Assign assets and resources to meet intelligence requirements
E5	CORE	Compile collection metrics
E4	CORE	Comply with Intelligence Oversight (IO) requirements
E5	NON-CORE	Conduct Intelligence Preparation of the Operating Environment (IPOE)
E5	NON-CORE	Conduct Joint Intelligence Preparation of the Operational Environment (JIPOE)
E7	NON-CORE	Construct collection matrix
E7	CORE	Construct collection plans
E6	CORE	Coordinate available intelligence resources
E7	CORE	Coordinate Concept of Operations (CONOPS) through Battleforce Stakeholders
E5	CORE	Coordinate geolocation operations
E7	CORE	Coordinate mission operations
E7	CORE	Coordinate Signals Intelligence (SIGINT) Indications and Warnings (I&W)
E7	CORE	Create cryptologic tasking for mission requirements
E7	CORE	Cross-check Intelligence Requirements (IR)
E5	NON-CORE	Deconflict frequency usage
E5	CORE	Determine collection gaps
E6	CORE	Determine collection requirements
E7	CORE	Determine intelligence gaps
E5	NON-CORE	Develop communications Electronic Attack (EA) briefs
E7	CORE	Direct Signals Intelligence (SIGINT) taskings
E7	CORE	Draft Signals Intelligence (SIGINT) operations policies and procedures
E6	CORE	Enforce compliance with Intelligence Oversight (IO) requirements
E5	NON-CORE	Establish communications infrastructure for data exfiltration
E7	CORE	Evaluate collection metrics
E4	CORE	Identify information flow within the intelligence cycle (Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED))
E4	CORE	Implement United States Signals Intelligence Directives (USSID)

INTELLIGENCE PLANNING AND DIRECTION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Incorporate Commanders Critical Information Requirements (CCIRs) to include priority intelligence requirements (PIR) into collection management activities
E7	CORE	Incorporate National Intelligence Priorities Framework (NIPF)
E7	CORE	Integrate Signals Intelligence (SIGINT) resources
E6	NON-CORE	Manage accesses on a Mission Correlation Table (MCT)
E6	NON-CORE	Manage Afloat Direction Finding Control (ADFC)
E7	CORE	Manage Critical (CRITIC) message programs
E7	CORE	Manage Cryptologic Carry-on (CCOP) systems
E6	NON-CORE	Manage cyberspace taskings
E7	CORE	Manage Information Related Capability (IRC) programs
E7	CORE	Manage intelligence support solutions
E6	NON-CORE	Manage Radio Frequency (RF) propagation modeling
E7	CORE	Manage remote access capabilities
E7	CORE	Manage Signals Intelligence (SIGINT) and cyber mission requirement resources
E5	NON-CORE	Perform database auditing
E7	CORE	Prioritize Intelligence Requirements (IR)
E4	CORE	Produce area of interest briefs
E6	CORE	Provide coordination, validation, and management assistance of Signals Intelligence (SIGINT) collection requirements, plans, and/or activities
E5	CORE	Provide target nomination recommendations which meet commander's objectives
E4	CORE	Research military Order of Battle (OOB)
E4	CORE	Research Signals Intelligence (SIGINT) Order of Battle (OOB)
E7	CORE	Submit Cryptologic capabilities requirements for implementation and mission sustainment
E6	CORE	Submit priority recommendations to support Commander's Critical Information Requirements (CCIR)
E5	CORE	Supervise Intelligence, Surveillance, and Reconnaissance (ISR) operations
E5	NON-CORE	Support Communications Security Material System (CMS) Operations
E7	CORE	Validate Collection Management Authority (CMA) requirements in support of Intelligence, Surveillance and Reconnaissance (ISR) Concept of Operations (CONOPS)

INTELLIGENCE PROCESSING AND EXPLOITATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Analyze modems
E4	CORE	Analyze multiple access schemes
E4	CORE	Analyze wireless communications for exploitation
E5	NON-CORE	Assess collateral effects of targeting operations
E4	CORE	Convert numbering systems
E4	CORE	Correlate case notations

INTELLIGENCE PROCESSING AND EXPLOITATION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Demodulate basic signals
E4	CORE	Detect bit synchronizers
E4	CORE	Determine Communication Emitter Notations (CENOT)
E4	CORE	Determine Linear Recursive Sequences (LRS)
E4	CORE	Determine short duration and non-communications signals
E4	CORE	Forward digitized signals
E4	NON-CORE	Identify Communication External Notations (COMEXT)
E4	CORE	Identify Foreign Instrumentation Signals Intelligence (FISINT) to meet mission requirements
E4	CORE	Identify PROFORMA to meet mission requirements
E4	CORE	Perform File Transfer Protocol (FTP)
E4	NON-CORE	Perform track management and target identification
E4	CORE	Perform waveform analysis
E4	CORE	Perform wavelength to frequency conversions
E4	CORE	Process Signals of Interest (SOI)
E4	CORE	Verify internal signal structures

NETWORK EXPLOITATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Conduct proximal access network operations
E5	NON-CORE	Perform packet capture (PCAP) analysis
E4	CORE	Process digital network communications

TRAINING

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Conduct Combat Systems Training Team (CSTT) drills
E7	CORE	Conduct operational certifications
E5	NON-CORE	Implement Command Readiness Training Team (CRTT)

Job Title

Cyber Analyst And Reporter

Job Code

002807

Job Family

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

CYBER ANALYST AND REPORTER

Short Title (14 Characters)

CYBER ANALYST

Pay Plan

Enlisted

Career Field

CTR

Other Relationships and Rules

NECs CXXX series and other NECs as assigned

Job Description

Cyber Analysts and Reporters perform cyberspace target development, discovery, and reporting in support of Cyberspace Operations to meet special operations forces, National, Fleet, and Joint requirements; and control and safeguard classified information to include storage, transportation, and protection.

DoD Relationship

Group Title

Analysis Specialists

DoD Code

123200

O*NET Relationship

Occupation Title

Computer Network Architects

SOC Code

15-1241.00

Job Family

Computer and Mathematical

Skills

Critical Thinking

Complex Problem Solving

Reading Comprehension

Judgment and Decision Making

Management of Material Resources

Systems Analysis

Coordination

Operation and Control

Science

Writing

Abilities

Deductive Reasoning

Inductive Reasoning

Written Comprehension

Information Ordering

Written Expression

Speed of Closure

Category Flexibility

Perceptual Speed

Oral Expression

Problem Sensitivity

FIREPOWER EMPLOYMENT

Paygrade

E5

Task Type

NON-CORE

Task Statements

Assess Measures of Performance (MOP)

E4

CORE

Comply with current communications Electronic Warfare (EW) Rules of Engagement (ROE)

E5

NON-CORE

Conduct Battle Damage Assessments (BDA)

E5

NON-CORE

Conduct Counter-Unmanned Aerial Systems (C-UAS) operations

E6

NON-CORE

Evaluate Measures of Effectiveness (MOE)

FORCE PROTECTION

Paygrade

E4

Task Type

CORE

Task Statements

Control access to restricted areas

E4

CORE

Destroy Sensitive Compartmented Information (SCI) materials

E4

CORE

Document receipt of classified materials

E7

CORE

Enforce Operations Security (OPSEC)

E4

CORE

Implement Emergency Action Plans (EAP)

E7

NON-CORE

Manage Sensitive Compartmented Information Facility (SCIF) accreditations

E4

CORE

Perform Counter-Intelligence, Surveillance, and Reconnaissance (C-ISR)

E4

CORE

Properly mark Sensitive Compartmented Information (SCI) materials

E4

CORE

Report Electronic Attack (EA) against friendly units, systems, links or nodes

E4

CORE

Safeguard Sensitive Compartmented Information (SCI) materials

E4

CORE

Transport Sensitive Compartmented Information (SCI) materials

INFORMATION OPERATION SUPPORT

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	NON-CORE	Provide cyber support to Electronic Warfare (EW) operations

INTELLIGENCE ANALYSIS AND PRODUCTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Analyze collection sources
E5	NON-CORE	Analyze Command, Control, Communications, Computers, Cyberspace, Intelligence, Surveillance, Reconnaissance, and Target (C5ISRT) networks for critical nodes
E4	NON-CORE	Analyze communication device capabilities
E5	NON-CORE	Analyze network intrusion global threat activity data
E5	NON-CORE	Analyze network vulnerabilities
E5	CORE	Analyze PROFORMA to meet mission requirements
E4	NON-CORE	Determine intelligence document source
E5	CORE	Develop Area of Responsibility (AOR) target data
E5	NON-CORE	Develop cyber persona profiles
E5	NON-CORE	Develop pattern of life analysis
E5	CORE	Develop target packages
E5	CORE	Develop target profiles
E5	CORE	Develop targets in support of commander's intent
E4	NON-CORE	Draft intelligence product reports
E5	CORE	Draft post-mission reports
E5	NON-CORE	Edit serialized intelligence reports for dissemination
E6	NON-CORE	Evaluate adversary critical capabilities, requirements, and vulnerabilities
E5	NON-CORE	Identify adversary critical capabilities, requirements, and vulnerabilities
E5	CORE	Identify adversary Tactics, Techniques, and Procedures (TTP)
E5	NON-CORE	Perform asset source validation
E4	NON-CORE	Perform Boolean and lucene logic
E4	CORE	Perform content analysis
E4	CORE	Perform geolocation analysis
E5	NON-CORE	Perform media analysis (e.g., memory, phones, physical devices, etc.)
E4	CORE	Perform metadata analysis
E5	NON-CORE	Perform non-traditional targeting operations
E4	NON-CORE	Perform Signals Intelligence (SIGINT) Geospatial Analysis (SGA)
E4	CORE	Perform Signals Intelligence (SIGINT) research using Intelligence Community (IC) databases to meet mission requirements
E5	NON-CORE	Perform technical target analysis
E4	CORE	Perform traffic analysis
E5	NON-CORE	Perform Unattended Ground Sensor (UGS) analysis
E5	NON-CORE	Perform untethered analysis
E5	CORE	Produce target communications profiles using technical data

INTELLIGENCE ANALYSIS AND PRODUCTION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Provide target Positive Identification (PID)
E6	NON-CORE	Release serialized intelligence reports for dissemination
E5	CORE	Research network technologies
E4	CORE	Respond to Request For Information (RFI)
E5	CORE	Review time sensitive reports
E6	NON-CORE	Validate technical aspects of cyberspace operations products

INTELLIGENCE AND DATA COLLECTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Assess Indication & Warning (I&W) threats
E4	CORE	Conduct wireless surveys
E5	NON-CORE	Create Signal Descriptor Files (SDF)
E7	NON-CORE	Determine capabilities of cyber assets relevant to specific target area
E6	NON-CORE	Develop automation processes
E4	NON-CORE	Employ specialized cyberspace tools to process data for analytic problems
E4	CORE	Execute commands within various Operating Systems (OS)
E4	CORE	Generate Request For Information (RFI)
E4	NON-CORE	Identify traffic source for targeting
E5	NON-CORE	Input information to mission databases and collection repositories for cyberspace operations
E4	CORE	Maintain target lists (e.g., Regional Target List (RTL), Joint Target List (JTL), Combined Target List (CTL))
E7	NON-CORE	Manage Command Readiness Training Team (CRTT)
E6	CORE	Manage geolocation operations
E5	NON-CORE	Perform Radio Frequency (RF) propagation modeling
E4	CORE	Perform remote access operations
E4	NON-CORE	Perform survey of Computer Network Operations (CNO) collection capabilities
E5	NON-CORE	Perform tactical Signals Intelligence (SIGINT) Intelligence, Surveillance, and Reconnaissance (ISR)
E5	NON-CORE	Perform untethered collections
E5	CORE	Provide feedback to developers on signals collection, processing, and analysis tools to mitigate existing shortfalls
E4	CORE	Review equipment status
E4	CORE	Troubleshoot system equipment failures and errors
E4	CORE	Troubleshoot system software failures and errors
E5	CORE	Verify collected information meets intelligence needs

INTELLIGENCE INTEGRATION AND DISSEMINATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	CORE	Brief intelligence operations
E4	CORE	Brief Signal Intelligence (SIGINT) Operations and capabilities
E5	CORE	Coordinate target analysis with external units
E6	CORE	Evaluate analysis and reporting operations
E7	CORE	Manage dissemination of Signals Intelligence (SIGINT) reports
E4	CORE	Provide Indications and Warnings (I&W) to tactical commanders
E5	CORE	Provide Time Sensitive Target (TST) operations intelligence support
E5	CORE	Sanitize cryptologic data for dissemination

INTELLIGENCE PLANNING AND DIRECTION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E6	CORE	Analyze collection metrics
E7	CORE	Assign assets and resources to meet intelligence requirements
E7	NON-CORE	Collaborate with Defensive Cyber Operations - Response Action (DCO-RA) / Offensive Cyber Operations (OCO) partners and consumers for mission requirements
E5	NON-CORE	Collaborate with Intelligence Community (IC) analysts for cyberspace operations
E5	CORE	Compile collection metrics
E4	CORE	Comply with Intelligence Oversight (IO) requirements
E5	NON-CORE	Conduct Intelligence Preparation of the Operating Environment (IPOE)
E5	NON-CORE	Conduct Joint Intelligence Preparation of the Operational Environment (JIPOE)
E7	CORE	Coordinate Concept of Operations (CONOPS) through Battleforce Stakeholders
E7	NON-CORE	Coordinate Cyberspace Operational Preparation of Environment (C-OPE) for mission requirements
E7	NON-CORE	Coordinate cyberspace operations with Special Access Program (SAP)/Integrated Joint Special Technical Operations (IJSTO) planners/Review and Approval Process for Cyber Operations (RAPCO)
E5	CORE	Coordinate geolocation operations
E7	CORE	Coordinate mission operations
E7	CORE	Coordinate Signals Intelligence (SIGINT) Indications and Warnings (I&W)
E5	NON-CORE	Coordinate target vetting with appropriate partners
E5	NON-CORE	Deconflict network operations
E5	CORE	Determine collection gaps
E6	CORE	Determine collection requirements
E7	CORE	Determine intelligence gaps
E7	CORE	Develop Cyberspace data acquisition plans
E5	NON-CORE	Develop target templates
E7	CORE	Direct Signals Intelligence (SIGINT) taskings
E7	CORE	Draft Signals Intelligence (SIGINT) operations policies and procedures
E6	CORE	Enforce compliance with Intelligence Oversight (IO) requirements

INTELLIGENCE PLANNING AND DIRECTION (CONT'D)

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Establish communications infrastructure for data exfiltration
E7	CORE	Evaluate collection metrics
E4	CORE	Identify information flow within the intelligence cycle (Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED))
E4	NON-CORE	Identify limitations of cyberspace tools, techniques and analytics
E5	NON-CORE	Identify remote physical targets for cyberspace capability pre-positioning
E5	NON-CORE	Identify remote virtual targets for cyberspace capability pre-positioning
E4	CORE	Implement United States Signals Intelligence Directives (USSID)
E7	CORE	Incorporate Commanders Critical Information Requirements (CCIRs) to include priority intelligence requirements (PIR) into collection management activities
E7	CORE	Incorporate National Intelligence Priorities Framework (NIPF)
E6	NON-CORE	Integrate cyberspace targeting efforts with other organization and combatant commands
E7	CORE	Integrate Signals Intelligence (SIGINT) resources
E6	NON-CORE	Manage accesses on a Mission Correlation Table (MCT)
E7	CORE	Manage Critical (CRITIC) message programs
E7	NON-CORE	Manage cyberspace analytic capabilities
E6	NON-CORE	Manage cyberspace taskings
E6	NON-CORE	Manage Radio Frequency (RF) propagation modeling
E7	CORE	Manage Signals Intelligence (SIGINT) and cyber mission requirement resources
E7	CORE	Manage targeting cycles
E5	NON-CORE	Perform database auditing
E6	NON-CORE	Perform predictive analysis of adversary actions in cyberspace
E7	CORE	Prioritize Intelligence Requirements (IR)
E6	NON-CORE	Provide coordination, validation, and management assistance of intelligence collection requirements, plans, and/or activities
E6	CORE	Provide coordination, validation, and management assistance of Signals Intelligence (SIGINT) collection requirements, plans, and/or activities
E4	NON-CORE	Provide input to cyberspace Concept of Operations (CONOPs)
E5	CORE	Provide target nomination recommendations which meet commander's objectives
E4	CORE	Research military Order of Battle (OOB)
E4	CORE	Research Signals Intelligence (SIGINT) Order of Battle (OOB)
E7	CORE	Submit Cryptologic capabilities requirements for implementation and mission sustainment
E6	CORE	Submit priority recommendations to support Commander's Critical Information Requirements (CCIR)
E5	CORE	Supervise Intelligence, Surveillance, and Reconnaissance (ISR) operations
E7	CORE	Validate Collection Management Authority (CMA) requirements in support of Intelligence, Surveillance and Reconnaissance (ISR) Concept of Operations (CONOPS)
E5	CORE	Verify mission taskings

INTELLIGENCE PROCESSING AND EXPLOITATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E4	NON-CORE	Analyze wireless communications for targeting
E5	NON-CORE	Assess collateral effects of targeting operations
E5	NON-CORE	Develop scripts and programs
E5	NON-CORE	Perform Counter-Unmanned Aerial Systems (C-UAS) analysis
E4	CORE	Perform File Transfer Protocol (FTP)
E4	CORE	Perform target exploitation operations

NETWORK EXPLOITATION

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E5	NON-CORE	Analyze common system services
E4	NON-CORE	Analyze digital network communications
E5	NON-CORE	Analyze known and non-standard protocols
E5	NON-CORE	Analyze network device configurations
E5	NON-CORE	Analyze network security architecture components
E5	NON-CORE	Analyze network traffic to identify anomalous activity and potential threats
E4	NON-CORE	Analyze Operating System (OS) characteristics for cyberspace operations
E4	NON-CORE	Analyze software and hardware for cyberspace operations
E5	NON-CORE	Analyze system, event, and network logs
E4	NON-CORE	Analyze target implementation of digital network technologies and systems
E5	NON-CORE	Conduct mid-point analysis (e.g., routers, firewalls, etc.)
E5	NON-CORE	Coordinate forensic processes
E5	NON-CORE	Detect network vulnerabilities
E5	NON-CORE	Determine basic structure and architecture of networks
E5	NON-CORE	Determine Operating System (OS) characteristics
E5	NON-CORE	Determine software and hardware vulnerabilities
E6	NON-CORE	Evaluate information networks defensive posture of target networks
E6	NON-CORE	Evaluate Mission Relevant Terrain-Cyber (MRTC)
E5	NON-CORE	Identify access vectors for networks of interest
E4	NON-CORE	Identify target communications within the global network
E4	NON-CORE	Identify the functions of a target's network elements
E5	NON-CORE	Map digital networks
E5	NON-CORE	Perform file system analysis
E5	NON-CORE	Perform packet capture (PCAP) analysis
E4	NON-CORE	Perform protocol analysis
E5	NON-CORE	Perform website characterizations
E4	CORE	Process digital network communications

TRAINING

<u>Paygrade</u>	<u>Task Type</u>	<u>Task Statements</u>
E7	CORE	Conduct operational certifications
E5	NON-CORE	Implement Command Readiness Training Team (CRTT)
E7	NON-CORE	Support wargaming for Computer Network Operations (CNO)