

CHAPTER 20



CRYPTOLOGIC TECHNICIAN (CT)

NAVPERS 18068-20L
CHG-75

TABLE OF CONTENTS
CRYPTOLOGIC TECHNICIAN (NETWORKS) (CTN)

| | |
|---|--------|
| SCOPE OF RATING | CTN-4 |
| GENERAL INFORMATION | CTN-5 |
| CRYPTOLOGIC CYBERSPACE RESEARCH AND DEVELOPMENT SPECIALIST | CTN-6 |
| CYBER DEVELOPMENT AND EVALUATION | CTN-6 |
| CYBER PLANNING | CTN-7 |
| CYBERSPACE OPERATIONS | CTN-7 |
| FORENSIC ANALYSIS | CTN-7 |
| SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION | CTN-7 |
| SYSTEMS ANALYSIS | CTN-8 |
| TARGET DEVELOPMENT | CTN-8 |
| VULNERABILITY ANALYSIS | CTN-8 |
| CRYPTOLOGIC CYBERSPACE ANALYST | CTN-9 |
| CYBER DEVELOPMENT AND EVALUATION | CTN-9 |
| CYBER PLANNING | CTN-9 |
| CYBERSPACE OPERATIONS | CTN-10 |
| FORENSIC ANALYSIS | CTN-11 |
| SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION | CTN-11 |
| SYSTEMS ANALYSIS | CTN-11 |
| TARGET DEVELOPMENT | CTN-12 |
| VULNERABILITY ANALYSIS | CTN-12 |
| CRYPTOLOGIC CYBERSPACE PLANNER | CTN-13 |
| CYBER DEVELOPMENT AND EVALUATION | CTN-13 |
| CYBER PLANNING | CTN-13 |
| CYBERSPACE OPERATIONS | CTN-14 |
| SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION | CTN-15 |
| SYSTEMS ANALYSIS | CTN-15 |
| TARGET DEVELOPMENT | CTN-15 |
| VULNERABILITY ANALYSIS | CTN-15 |
| CRYPTOLOGIC CYBERSPACE OPERATOR | CTN-16 |
| CYBER DEVELOPMENT AND EVALUATION | CTN-16 |
| CYBER PLANNING | CTN-16 |
| CYBERSPACE OPERATIONS | CTN-17 |
| FORENSIC ANALYSIS | CTN-18 |
| SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION | CTN-18 |
| SYSTEMS ANALYSIS | CTN-18 |

TARGET DEVELOPMENT
VULNERABILITY ANALYSIS

CTN-18

CTN-19

CTN-3

NAVY ENLISTED OCCUPATIONAL STANDARD
FOR
CRYPTOLOGIC TECHNICIAN (NETWORKS) (CTN)



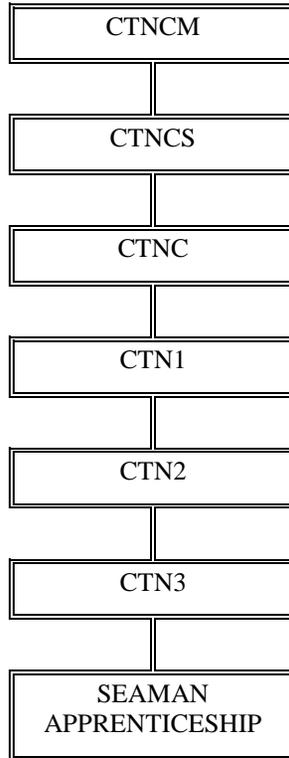
SCOPE OF RATING

Cryptologic Technicians (Networks) (CTN) employ tactical and strategic capabilities to plan, develop, and execute offensive and defensive Cyberspace Operations; perform Cyber Defense, Digital Forensics, Network Exploitation, Research and Development, and Cyber Planning; leverage tactical and strategic signals intelligence and cryptologic functions; produce and execute cyber effects; identify and report worldwide threats in support of special operations forces, and national, fleet, and joint requirements; and control and safeguard access to classified material and information systems.

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 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 additional 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**Cryptologic Cyberspace Research and Development Specialist****Job Code****002775****Job Family**

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

CRYPTOLOGIC CYBERSPACE R&D SPC

Short Title (14 Characters)

CRYPTO CYB R&D

Pay Plan

Enlisted

Career Field

CTN

Other Relationships and Rules

NEC's as assigned

Job Description

Cryptologic Cyberspace Research and Development Specialists conduct software and systems engineering; conduct systems research to develop new capabilities in support of offensive and defensive cyber missions for special operations forces, national, fleet, and joint requirements; and conduct comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

DoD Relationship**Group Title**

Analysis

DoD Code

123200

O*NET Relationship**Occupation Title**Computer and Information
Research Scientists**SOC Code**

15-1111.00

Job Family

Computer and Mathematical

Skills

Critical Thinking
Systems Analysis
Complex Problem Solving
Mathematics
Quality Control Analysis
Judgment and Decision Making
Programming
Systems Evaluation
Reading Comprehension
Operations Analysis

Abilities

Written Expression
Selective Attention
Deductive Reasoning
Written Comprehension
Inductive Reasoning
Information Ordering
Originality
Mathematical Reasoning
Oral Comprehension
Oral Expression

CYBER DEVELOPMENT AND EVALUATION**Paygrade****Task Type****Task Statements**

| | | |
|----|----------|---|
| E6 | NON-CORE | Collaborate with stakeholders for defensive cyber tools |
| E4 | NON-CORE | Configure virtualized development environments |
| E5 | NON-CORE | Create algorithms to solve complex problems |
| E5 | NON-CORE | Develop capabilities using compiled and assembled languages |
| E4 | CORE | Develop capabilities using scripting languages |
| E5 | NON-CORE | Develop cyberspace operations tools and platforms |
| E5 | NON-CORE | Develop defensive cyber tools |
| E7 | NON-CORE | Evaluate cyberspace operations software tools, capabilities, and platforms |
| E5 | NON-CORE | Interpret assembly code |
| E4 | CORE | Interpret source code |
| E5 | NON-CORE | Maintain cyberspace operations tools, capabilities, and platforms |
| E7 | NON-CORE | Perform advanced reverse engineering of binaries |
| E5 | NON-CORE | Perform basic reverse engineering of binaries |
| E4 | CORE | Perform boolean logic |
| E4 | CORE | Perform discrete math functions |
| E6 | NON-CORE | Perform intermediate reverse engineering of binaries |
| E5 | NON-CORE | Validate cyberspace operations software tools, capabilities, and platforms Operational Test and Evaluate (OTE) |
| E7 | NON-CORE | Validate requirements for defensive cyber tools |

CYBER PLANNING

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|--|
| E6 | CORE | Analyze data (e.g. Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.) |
| E7 | CORE | Assess strategic impacts of tools and techniques on specific targets |
| E7 | CORE | Evaluate technical aspects of organic products (e.g. reports, working aids, Concept of Operations (CONOPS), etc.) |
| E6 | CORE | Identify Intelligence gaps |
| E7 | CORE | Perform cyberspace assessments |

CYBERSPACE OPERATIONS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|---|
| E5 | NON-CORE | Analyze Signals of Interest (SOI) |
| E5 | CORE | Assess impact of Tactics, Techniques, and Procedures (TTP) on a target |
| E4 | CORE | Assess operational environment |
| E5 | NON-CORE | Conduct Operation, Test, and Evaluation (OTE) of Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS) |
| E7 | CORE | Coordinate with Offensive Cyber Operations (OCO)/Defensive Cyber Operations (DCO) partners and stakeholders |
| E4 | CORE | Detect network vulnerabilities |
| E5 | NON-CORE | Fabricate collection and exploitation equipment (Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS)) |
| E5 | NON-CORE | Perform Operational Test and Evaluation (OTE) of cyber tools |
| E5 | CORE | Prepare technical aspects of organic products (e.g. reports, working aids, Concept of Operations (CONOPS), etc.) |
| E5 | CORE | Provide technical solutions from all source data (e.g. Signals Intelligence (SIGINT), network data, etc.) |
| E4 | CORE | Verify operational authorities |

FORENSIC ANALYSIS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|---|
| E4 | NON-CORE | Perform basic media forensic analysis |
| E5 | NON-CORE | Perform behavioral malware analysis |
| E6 | NON-CORE | Perform in-depth malware analysis and reverse engineering |
| E5 | NON-CORE | Perform intermediate media analysis (e.g. memory, phones, physical devices, etc.) |
| E4 | CORE | Perform triage malware analysis |

SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|--|
| E6 | NON-CORE | Coordinate Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations |
| E4 | CORE | Destroy Sensitive Compartmented Information (SCI) materials |
| E6 | CORE | Document receipt of Sensitive Compartmented Information (SCI) materials |
| E4 | CORE | Implement Emergency Action Plans (EAP) |
| E4 | CORE | Inventory Sensitive Compartmented Information (SCI) materials |

SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION (CONT'D)

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|--|
| E7 | NON-CORE | Manage Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations |
| E4 | CORE | Safeguard Sensitive Compartmented Information (SCI) materials |
| E4 | CORE | Store Sensitive Compartmented Information (SCI) materials |

SYSTEMS ANALYSIS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|--|
| E4 | CORE | Analyze common system services |
| E4 | CORE | Analyze file systems (e.g. file structures, hierarchies, management, etc.) |
| E4 | CORE | Analyze network security architecture components |
| E4 | CORE | Analyze Operating System (OS) characteristics |
| E4 | CORE | Analyze raw data (e.g. Signals Intelligence (SIGINT), network, wireless, etc.) |
| E4 | CORE | Analyze remote system environments |
| E4 | CORE | Analyze software and hardware |

TARGET DEVELOPMENT

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|--|
| E4 | CORE | Analyze metadata |
| E4 | CORE | Compile multiple source data |
| E5 | NON-CORE | Construct virtualized network based on target data |
| E5 | NON-CORE | Develop Pattern of Life (POL) analysis |
| E5 | NON-CORE | Perform asset validation |

VULNERABILITY ANALYSIS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|---------------------------------------|
| E5 | CORE | Assess target network vulnerabilities |

Job Title**Cryptologic Cyberspace Analyst****Job Code****003006****Job Family**

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

CRYPTOLOGIC CYBERSPACE ANALYST

Short Title (14 Characters)

CRYPTO CYB ANL

Pay Plan

Enlisted

Career Field

CTN

Other Relationships and Rules

NEC's as assigned

Job Description

Cryptologic Cyberspace Analysts conduct analysis in support of offensive and defensive cyberspace operations to meet special operations forces, national, fleet, and joint requirements; and perform cyberspace target development and exploitation analysis, Indications and Warning (I&W), Attack Sensing and Warning (AS&W), forensic analysis, discovery, and counter-infiltration.

DoD Relationship**Group Title**

Analysis

DoD Code

123200

O*NET Relationship**Occupation Title**

Computer Network Support Specialists

SOC Code

15-1152.00

Job Family

Computer and Mathematical

Skills

Critical Thinking
Complex Problem Solving
Judgment and Decision Making
Systems Analysis
Operations Analysis
Reading Comprehension
Quality Control Analysis
Systems Evaluation
Mathematics
Coordination

Abilities

Written Expression
Deductive Reasoning
Inductive Reasoning
Selective Attention
Information Ordering
Written Comprehension
Originality
Problem Sensitivity
Oral Expression
Mathematical Reasoning

CYBER DEVELOPMENT AND EVALUATION**Paygrade****Task Type****Task Statements**

| | | |
|----|----------|--|
| E4 | NON-CORE | Configure virtualized development environments |
| E4 | CORE | Develop capabilities using scripting languages |
| E7 | NON-CORE | Evaluate cyberspace operations software tools, capabilities, and platforms |
| E5 | NON-CORE | Interpret assembly code |
| E4 | CORE | Interpret source code |
| E5 | NON-CORE | Maintain cyberspace operations tools, capabilities, and platforms |
| E7 | NON-CORE | Perform advanced reverse engineering of binaries |
| E5 | NON-CORE | Perform basic reverse engineering of binaries |
| E4 | CORE | Perform boolean logic |
| E4 | CORE | Perform discrete math functions |
| E6 | NON-CORE | Perform intermediate reverse engineering of binaries |

CYBER PLANNING**Paygrade****Task Type****Task Statements**

| | | |
|----|------|--|
| E6 | CORE | Analyze data (e.g. Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.) |
| E6 | CORE | Assess event data to support Commander's Critical Information Requirements (CCIR) objectives |
| E7 | CORE | Assess strategic impacts of tools and techniques on specific targets |
| E6 | CORE | Conduct mission analysis |

CYBER PLANNING (CONT'D)

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|---|
| E7 | CORE | Coordinate cyberspace operations with Intelligence Community (IC) stakeholders |
| E7 | CORE | Coordinate cyberspace operations with stakeholders |
| E7 | CORE | Deliver target development recommendations |
| E7 | CORE | Develop cyberspace-related plans (e.g. Operation Plan (OPLAN), Concept of Operations Plan (CONPLAN), Concept of Operations (CONOP), etc.) |
| E6 | CORE | Develop cyberspace-related Tactics, Techniques, and Procedures (TTP) |
| E5 | NON-CORE | Develop offensive cyber Operations Plans (OPLAN) |
| E7 | CORE | Evaluate technical aspects of organic products (e.g. reports, working aids, Concept of Operations (CONOPS), etc.) |
| E6 | CORE | Identify Intelligence gaps |
| E6 | CORE | Manage collection requirements |
| E7 | CORE | Perform cyberspace assessments |
| E6 | NON-CORE | Perform operational and tactical deconfliction |
| E6 | CORE | Recommend targets based on all source reporting |
| E7 | NON-CORE | Respond to formal Requests for Information (RFI) |
| E7 | CORE | Respond to operational and tactical deconfliction requests |
| E7 | CORE | Validate collection requirements |

CYBERSPACE OPERATIONS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|---|
| E5 | NON-CORE | Analyze Signals of Interest (SOI) |
| E5 | CORE | Assess impact of Tactics, Techniques, and Procedures (TTP) on a target |
| E4 | CORE | Assess operational environment |
| E4 | CORE | Collect network data |
| E5 | CORE | Communicate with Offensive Cyber Operations (OCO)/Defensive Cyber Operations (DCO) partners and stakeholders |
| E4 | CORE | Conduct Defensive Cyberspace Operations (DCO) |
| E5 | CORE | Conduct network surveys |
| E5 | NON-CORE | Conduct Operation, Test, and Evaluation (OTE) of Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS) |
| E7 | CORE | Coordinate with Offensive Cyber Operations (OCO)/Defensive Cyber Operations (DCO) partners and stakeholders |
| E4 | CORE | Detect network vulnerabilities |
| E5 | CORE | Evaluate collection requirements |
| E5 | CORE | Evaluate raw data (e.g. Signals Intelligence (SIGINT), network, wireless, etc.) |
| E5 | CORE | Evaluate remote system environments |
| E5 | NON-CORE | Evaluate remote targets for pre-positioning |
| E5 | NON-CORE | Fabricate collection and exploitation equipment (Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS)) |
| E5 | NON-CORE | Perform untethered collections |

CYBERSPACE OPERATIONS (CONT'D)

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|---|
| E5 | CORE | Prepare technical aspects of organic products (e.g. reports, working aids, Concept of Operations (CONOPS), etc.) |
| E5 | CORE | Provide technical solutions from all source data (e.g. Signals Intelligence (SIGINT), network data, etc.) |
| E5 | NON-CORE | Provide time sensitive geolocation information. |
| E4 | CORE | Provide time sensitive reporting information (e.g. Critical Intelligence Communication (CRITIC), Commanders Critical Information Requirements (CCIRs), voice reports, etc.) |
| E4 | CORE | Report time sensitive information |
| E4 | CORE | Verify operational authorities |

FORENSIC ANALYSIS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|---|
| E5 | CORE | Document forensic processes and evidence collection |
| E7 | NON-CORE | Manage forensic processes |
| E4 | NON-CORE | Perform basic media forensic analysis |
| E5 | NON-CORE | Perform behavioral malware analysis |
| E4 | CORE | Perform forensic data acquisition |
| E6 | NON-CORE | Perform in-depth malware analysis and reverse engineering |
| E5 | NON-CORE | Perform intermediate media analysis (e.g. memory, phones, physical devices, etc.) |
| E4 | CORE | Perform triage malware analysis |

SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|--|
| E4 | CORE | Control access to Sensitive Compartmented Information Facility (SCIF) |
| E6 | NON-CORE | Coordinate Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations |
| E4 | CORE | Destroy Sensitive Compartmented Information (SCI) materials |
| E6 | CORE | Document receipt of Sensitive Compartmented Information (SCI) materials |
| E4 | CORE | Implement Emergency Action Plans (EAP) |
| E4 | CORE | Inventory Sensitive Compartmented Information(SCI) materials |
| E7 | NON-CORE | Manage Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations |
| E4 | CORE | Safeguard Sensitive Compartmented Information (SCI) materials |
| E4 | CORE | Store Sensitive Compartmented Information (SCI) materials |

SYSTEMS ANALYSIS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|--|
| E4 | CORE | Analyze common system services |
| E4 | CORE | Analyze file systems (e.g. file structures, hierarchies, management, etc.) |
| E4 | CORE | Analyze network security architecture components |
| E4 | CORE | Analyze Operating System (OS) characteristics |
| E4 | CORE | Analyze raw data (e.g. Signals Intelligence (SIGINT), network, wireless, etc.) |

SYSTEMS ANALYSIS (CONT'D)

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|---|
| E4 | CORE | Analyze remote system environments |
| E4 | CORE | Analyze software and hardware |
| E4 | CORE | Determine basic structure and architecture of networks (e.g. wired, wireless, cellular, etc.) |
| E4 | CORE | Determine threat Tactics, Techniques, and Procedures (TTP) |

TARGET DEVELOPMENT

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|--|
| E4 | CORE | Analyze metadata |
| E4 | CORE | Analyze remote target network composition |
| E4 | NON-CORE | Analyze remote targets for pre-positioning |
| E5 | NON-CORE | Assess physical characteristics of the target environment |
| E4 | CORE | Compile multiple source data |
| E5 | NON-CORE | Construct virtualized network based on target data |
| E5 | CORE | Determine intelligence value |
| E4 | CORE | Develop network maps |
| E5 | NON-CORE | Develop Pattern of Life (POL) analysis |
| E4 | CORE | Develop target templates |
| E4 | CORE | Gather target information |
| E7 | NON-CORE | Manage unit priority target lists |
| E5 | NON-CORE | Perform asset validation |
| E5 | NON-CORE | Perform tactical Airborne Precision Geolocation (APGL) operations/Unmanned Aerial Systems (UAS) payload operations |
| E5 | NON-CORE | Perform tactical Precision Geolocation (PGL) |
| E5 | NON-CORE | Perform target geospatial analysis |
| E5 | CORE | Provide cyber Concept of Operations (CONOP) input |
| E5 | NON-CORE | Provide target Positive Identification (PID) |
| E4 | CORE | Verify target capabilities |

VULNERABILITY ANALYSIS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|--|
| E5 | CORE | Analyze network intrusion global threat activity data |
| E5 | CORE | Analyze threat Tactics, Techniques, and Procedures (TTP) |
| E5 | CORE | Assess target network vulnerabilities |
| E5 | CORE | Report current/emerging cyber threats, intrusions, incidents, and events |
| E7 | CORE | Validate target network vulnerabilities |

Job Title**Cryptologic Cyberspace Planner****Job Code****003103****Job Family**
Management**NOC**
TBD**Short Title (30 Characters)**
CRYPTOLOGIC CYBERSPACE PLANNER**Short Title (14 Characters)**
CRYPTO CYB PLN**Pay Plan**
Enlisted**Career Field**
CTN**Other Relationships and Rules**
NEC's as assigned**Job Description**

Cryptologic Cyberspace Planners perform in-depth targeting and cyber planning; conduct strategic, operational, and tactical level planning across the full range of operations for integrated information and cyberspace operations; compile information; and develop detailed plans and orders in support of special operations forces, joint, fleet, and national requirements.

DoD Relationship

| | |
|---------------------------|------------------------|
| <u>Group Title</u> | <u>DoD Code</u> |
| Analysis | 123200 |

O*NET Relationship

| | | |
|---|------------------------|--------------------------|
| <u>Occupation Title</u> | <u>SOC Code</u> | <u>Job Family</u> |
| Computer and Information Systems Managers | 11-3021.00 | Management |

Skills

Critical Thinking
 Judgment and Decision Making
 Coordination
 Complex Problem Solving
 Reading Comprehension
 Quality Control Analysis
 Systems Evaluation
 Monitoring
 Operations Analysis
 Active Listening

Abilities

Written Expression
 Deductive Reasoning
 Inductive Reasoning
 Oral Expression
 Information Ordering
 Written Comprehension
 Selective Attention
 Oral Comprehension
 Problem Sensitivity
 Originality

CYBER DEVELOPMENT AND EVALUATION

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|---|
| E6 | NON-CORE | Collaborate with stakeholders for defensive cyber tools |
| E7 | NON-CORE | Validate requirements for defensive cyber tools |

CYBER PLANNING

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|---|
| E6 | CORE | Analyze data (e.g. Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.) |
| E6 | CORE | Assess event data to support Commander's Critical Information Requirements (CCIR) objectives |
| E7 | CORE | Assess strategic impacts of tools and techniques on specific targets |
| E7 | NON-CORE | Conduct exercise planning |
| E6 | CORE | Conduct mission analysis |
| E7 | NON-CORE | Confirm authorities and Standing Rules of Engagement (SROE) for cyberspace operations planning |
| E7 | CORE | Coordinate cyberspace Operational Preparation of Environment (OPE) |
| E7 | CORE | Coordinate cyberspace operations with Intelligence Community (IC) stakeholders |
| E7 | NON-CORE | Coordinate cyberspace operations with Special Access Program (SAP)/Integrated Joint Special Technical Operations (IJSTO) planners |
| E7 | CORE | Coordinate cyberspace operations with stakeholders |

CYBER PLANNING (CONT'D)

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|---|
| E7 | NON-CORE | Coordinate Electronic Warfare (EW)/Cyber Operations with joint/allied partners |
| E6 | CORE | Coordinate legal compliance reviews |
| E5 | CORE | Deconflict scheduled network operations |
| E7 | CORE | Deliver target development recommendations |
| E7 | CORE | Develop cyberspace-related plans (e.g. Operation Plan (OPLAN), Concept of Operations Plan (CONPLAN), Concept of Operations (CONOP), etc.) |
| E6 | CORE | Develop cyberspace-related Tactics, Techniques, and Procedures (TTP) |
| E5 | NON-CORE | Develop offensive cyber Operations Plans (OPLAN) |
| E7 | CORE | Evaluate technical aspects of organic products (e.g. reports, working aids, Concept of Operations (CONOPS), etc.) |
| E6 | CORE | Identify Intelligence gaps |
| E7 | CORE | Integrate cyberspace planning efforts with stakeholders and combatant commands |
| E6 | CORE | Maintain deliberate and/or crisis action plans |
| E6 | CORE | Manage collection requirements |
| E7 | NON-CORE | Manage Electronic Warfare (EW)/Cyber Operations exercises |
| E7 | CORE | Perform cyberspace assessments |
| E6 | NON-CORE | Perform operational and tactical deconfliction |
| E6 | CORE | Recommend targets based on all source reporting |
| E6 | CORE | Report cyberspace effects (e.g. Measures of Performance (MOP), Measures of Effectiveness (MOE), and after action reports, etc.) |
| E7 | NON-CORE | Request supporting Electronic Warfare (EW)/Cyber Operations assets |
| E7 | NON-CORE | Respond to formal Requests for Information (RFI) |
| E7 | CORE | Respond to operational and tactical deconfliction requests |
| E7 | CORE | Validate collection requirements |

CYBERSPACE OPERATIONS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|--|
| E5 | CORE | Assess impact of Tactics, Techniques, and Procedures (TTP) on a target |
| E4 | CORE | Assess operational environment |
| E5 | CORE | Communicate with Offensive Cyber Operations (OCO)/Defensive Cyber Operations (DCO) partners and stakeholders |
| E7 | CORE | Coordinate with Offensive Cyber Operations (OCO)/Defensive Cyber Operations (DCO) partners and stakeholders |
| E5 | CORE | Evaluate collection requirements |
| E5 | CORE | Evaluate remote system environments |
| E5 | NON-CORE | Evaluate remote targets for pre-positioning |
| E5 | CORE | Prepare technical aspects of organic products (e.g. reports, working aids, Concept of Operations (CONOPS), etc.) |
| E5 | CORE | Provide technical solutions from all source data (e.g. Signals Intelligence (SIGINT), network data, etc.) |

CYBERSPACE OPERATIONS (CONT'D)

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|---|
| E4 | CORE | Provide time sensitive reporting information (e.g. Critical Intelligence Communication (CRITIC), Commanders Critical Information Requirements (CCIRs), voice reports, etc.) |
| E4 | CORE | Report time sensitive information |
| E4 | CORE | Verify operational authorities |

SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|--|
| E4 | CORE | Control access to Sensitive Compartmented Information Facility (SCIF) |
| E6 | NON-CORE | Coordinate Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations |
| E4 | CORE | Destroy Sensitive Compartmented Information (SCI) materials |
| E6 | CORE | Document receipt of Sensitive Compartmented Information (SCI) materials |
| E4 | CORE | Implement Emergency Action Plans (EAP) |
| E4 | CORE | Inventory Sensitive Compartmented Information (SCI) materials |
| E7 | NON-CORE | Manage Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations |
| E4 | CORE | Safeguard Sensitive Compartmented Information (SCI) materials |
| E4 | CORE | Store Sensitive Compartmented Information (SCI) materials |

SYSTEMS ANALYSIS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|--|
| E4 | CORE | Determine threat Tactics, Techniques, and Procedures (TTP) |

TARGET DEVELOPMENT

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|---|
| E4 | CORE | Compile multiple source data |
| E5 | CORE | Determine intelligence value |
| E5 | NON-CORE | Develop Pattern of Life (POL) analysis |
| E4 | CORE | Gather target information |
| E7 | NON-CORE | Manage unit priority target lists |
| E5 | CORE | Provide cyber Concept of Operations (CONOP) input |
| E4 | CORE | Verify target capabilities |

VULNERABILITY ANALYSIS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|---|
| E5 | CORE | Analyze network intrusion global threat activity data |
| E5 | CORE | Assess target network vulnerabilities |
| E7 | CORE | Validate target network vulnerabilities |

Job Title

Cryptologic Cyberspace Operator

Job Code

003303

Job Family

Computer and Mathematical

NOC

TBD

Short Title (30 Characters)

CRYPTOLOGIC CYBERSPACE OPR

Short Title (14 Characters)

CRYPTO CYB OPR

Pay Plan

Enlisted

Career Field

CTN

Other Relationships and Rules

NEC's as assigned

Job Description

Cryptologic Cyberspace Operators perform operations in support of offensive and defensive missions to meet special operations forces, national, fleet, and joint requirements; and perform exploitation and attack operations, software testing and evaluation, threat emulation, and intelligence collection; and access network operations.

DoD Relationship

Group Title

Analysis

DoD Code

123200

O*NET Relationship

Occupation Title

Computer Network Support Specialists

SOC Code

15-1152.00

Job Family

Computer and Mathematical

Skills

- Critical Thinking*
- Judgment and Decision Making*
- Complex Problem Solving*
- Systems Analysis*
- Systems Evaluation*
- Operations Analysis*
- Quality Control Analysis*
- Reading Comprehension*
- Mathematics*
- Equipment Selection*

Abilities

- Deductive Reasoning*
- Inductive Reasoning*
- Written Expression*
- Selective Attention*
- Written Comprehension*
- Information Ordering*
- Problem Sensitivity*
- Originality*
- Oral Expression*
- Mathematical Reasoning*

CYBER DEVELOPMENT AND EVALUATION

| <u>Pavgrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|---|
| E6 | NON-CORE | Collaborate with stakeholders for defensive cyber tools |
| E4 | NON-CORE | Configure virtualized development environments |
| E5 | NON-CORE | Develop capabilities using compiled and assembled languages |
| E4 | CORE | Develop capabilities using scripting languages |
| E5 | NON-CORE | Develop cyberspace operations tools and platforms |
| E7 | NON-CORE | Evaluate cyberspace operations software tools, capabilities, and platforms |
| E5 | NON-CORE | Interpret assembly code |
| E4 | CORE | Interpret source code |
| E5 | NON-CORE | Maintain cyberspace operations tools, capabilities, and platforms |
| E5 | NON-CORE | Perform basic reverse engineering of binaries |
| E4 | CORE | Perform boolean logic |
| E4 | CORE | Perform discrete math functions |
| E5 | NON-CORE | Validate cyberspace operations software tools, capabilities, and platforms Operational Test and Evaluate (OTE) |

CYBER PLANNING

| <u>Pavgrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|--|
| E6 | CORE | Analyze data (e.g. Battle Damage Assessment (BDA), Measures of Performance (MOP), Measures of Effectiveness (MOE), etc.) |
| E6 | CORE | Assess event data to support Commander's Critical Information Requirements (CCIR) objectives |

CYBER PLANNING (CONT'D)

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|---|
| E7 | CORE | Assess strategic impacts of tools and techniques on specific targets |
| E5 | CORE | Deconflict scheduled network operations |
| E6 | CORE | Develop cyberspace-related Tactics, Techniques, and Procedures (TTP) |
| E7 | CORE | Evaluate technical aspects of organic products (e.g. reports, working aids, Concept of Operations (CONOPS), etc.) |
| E7 | CORE | Perform cyberspace assessments |
| E6 | CORE | Report cyberspace effects (e.g. Measures of Performance (MOP), Measures of Effectiveness (MOE), and after action reports, etc.) |

CYBERSPACE OPERATIONS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|------------------------|-------------------------|---|
| E5 | NON-CORE | Analyze Signals of Interest (SOI) |
| E5 | CORE | Assess impact of Tactics, Techniques, and Procedures (TTP) on a target |
| E4 | CORE | Assess operational environment |
| E4 | CORE | Collect network data |
| E5 | NON-CORE | Conduct access operations |
| E6 | NON-CORE | Conduct Computer Network Attack (CNA) operations |
| E5 | CORE | Conduct Computer Network Exploitation (CNE) operations |
| E4 | CORE | Conduct Defensive Cyberspace Operations (DCO) |
| E5 | CORE | Conduct network surveys |
| E5 | NON-CORE | Conduct Operation, Test, and Evaluation (OTE) of Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS) |
| E4 | CORE | Detect network vulnerabilities |
| E5 | CORE | Evaluate raw data (e.g. Signals Intelligence (SIGINT), network, wireless, etc.) |
| E5 | CORE | Evaluate remote system environments |
| E5 | NON-CORE | Evaluate remote targets for pre-positioning |
| E5 | NON-CORE | Fabricate collection and exploitation equipment (Commercial Off The Shelf (COTS)/Government Off The Shelf (GOTS)) |
| E5 | CORE | Perform cyberspace Operational Preparation of Environment (OPE) |
| E5 | NON-CORE | Perform Operational Test and Evaluation (OTE) of cyber tools |
| E5 | NON-CORE | Perform untethered collections |
| E5 | CORE | Prepare technical aspects of organic products (e.g. reports, working aids, Concept of Operations (CONOPS), etc.) |
| E5 | CORE | Provide technical solutions from all source data (e.g. Signals Intelligence (SIGINT), network data, etc.) |
| E5 | NON-CORE | Provide time sensitive geolocation information. |
| E4 | CORE | Provide time sensitive reporting information (e.g. Critical Intelligence Communication (CRITIC), Commanders Critical Information Requirements (CCIRs), voice reports, etc.) |
| E4 | CORE | Report time sensitive information |
| E4 | CORE | Verify operational authorities |

FORENSIC ANALYSIS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|---|
| E4 | NON-CORE | Perform basic media forensic analysis |
| E5 | NON-CORE | Perform behavioral malware analysis |
| E4 | CORE | Perform forensic data acquisition |
| E6 | NON-CORE | Perform live forensic incident response |
| E4 | CORE | Perform triage malware analysis |

SENSITIVE COMPARTMENTED INFORMATION (SCI) PROTECTION

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|--|
| E4 | CORE | Control access to Sensitive Compartmented Information Facility (SCIF) |
| E6 | NON-CORE | Coordinate Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations |
| E4 | CORE | Destroy Sensitive Compartmented Information (SCI) materials |
| E6 | CORE | Document receipt of Sensitive Compartmented Information (SCI) materials |
| E4 | CORE | Implement Emergency Action Plans (EAP) |
| E4 | CORE | Inventory Sensitive Compartmented Information (SCI) materials |
| E7 | NON-CORE | Manage Temporary Sensitive Compartmented Information Facility (TSCIF) accreditations |
| E4 | CORE | Safeguard Sensitive Compartmented Information (SCI) materials |
| E4 | CORE | Store Sensitive Compartmented Information (SCI) materials |

SYSTEMS ANALYSIS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|---|
| E4 | CORE | Analyze common system services |
| E4 | CORE | Analyze file systems (e.g. file structures, hierarchies, management, etc.) |
| E4 | CORE | Analyze network security architecture components |
| E4 | CORE | Analyze Operating System (OS) characteristics |
| E4 | CORE | Analyze raw data (e.g. Signals Intelligence (SIGINT), network, wireless, etc.) |
| E4 | CORE | Analyze remote system environments |
| E4 | CORE | Analyze software and hardware |
| E4 | CORE | Determine basic structure and architecture of networks (e.g. wired, wireless, cellular, etc.) |
| E4 | CORE | Determine threat Tactics, Techniques, and Procedures (TTP) |

TARGET DEVELOPMENT

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|---|
| E4 | CORE | Analyze metadata |
| E4 | NON-CORE | Analyze remote targets for pre-positioning |
| E5 | NON-CORE | Assess physical characteristics of the target environment |
| E4 | CORE | Compile multiple source data |
| E5 | NON-CORE | Construct virtualized network based on target data |
| E4 | CORE | Develop network maps |
| E5 | NON-CORE | Develop Pattern of Life (POL) analysis |
| E4 | CORE | Gather target information |

TARGET DEVELOPMENT (CONT'D)

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|--|
| E7 | NON-CORE | Manage unit priority target lists |
| E5 | NON-CORE | Perform asset validation |
| E5 | NON-CORE | Perform tactical Airborne Precision Geolocation (APGL) operations/Unmanned Aerial Systems (UAS) payload operations |
| E5 | NON-CORE | Perform tactical Precision Geolocation (PGL) |
| E5 | NON-CORE | Perform target geospatial analysis |
| E5 | CORE | Provide cyber Concept of Operations (CONOP) input |
| E5 | NON-CORE | Provide target Positive Identification (PID) |
| E4 | CORE | Verify target capabilities |

VULNERABILITY ANALYSIS

| <u>Paygrade</u> | <u>Task Type</u> | <u>Task Statements</u> |
|-----------------|------------------|--|
| E5 | CORE | Analyze threat Tactics, Techniques, and Procedures (TTP) |
| E5 | CORE | Assess target network vulnerabilities |
| E5 | CORE | Report current/emerging cyber threats, intrusions, incidents, and events |
| E7 | CORE | Validate target network vulnerabilities |