CHAPTER 20

CRYPTOLOGIC TECHNICIAN (INTERPRETIVE) (CTI)

NAVPERS 18068F-20F
Change 101

Updated: January 2025

TABLE OF CONTENTS
CRYPTOLOGIC TECHNICIAN (INTERPRETIVE) (CTI)

NAVY ENLISTED OCCUPATIONAL STANDARD

FOR

CRYPTOLOGIC TECHNICIAN (INTERPRETIVE) (CTI)

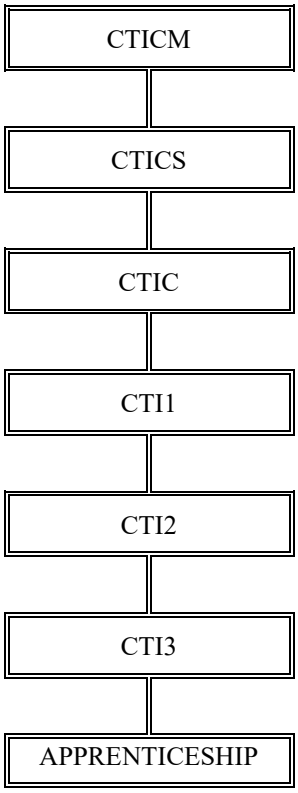
SCOPE OF RATING

Cryptologic Technicians (Interpretive) (CTI) specialize in foreign language, regional and cultural expertise, and advanced computer systems to support strategic, tactical, and cyberspace operations; collect, process, exploit, and analyze foreign language communications, digital network information, and Signals of Interest (SOI) to identify, monitor, and report global threats; translate and interpret foreign language materials; manage foreign language programs; provide regional and cultural guidance in support of National, Joint, Fleet (special operations, air, surface, and subsurface), and multi-national consumers and decision-makers; 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 18068E) 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.

Defense Language Proficiency Test (DLPT) Requirements. All candidates competing for paygrades E-4 (CTI3) through E-9 (CTICM) must achieve a current DLPT score of L2/R2 in the language that reflects their primary duty as determined by the member's commanding officer. Minimum proficiency of L2/R2 must be attained in order to be eligible for the next higher paygrade

SAFETY

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

Job Title **Job Code**

Strategic Language Analyst 001022

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Protective Service	TBD	STRATEGIC LANGUAGE ANALYST	STRAT LNGANLST

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	CTI	NEC CXXX and 7XXX series and other NECs as assigned

Job Description

Strategic Language Analysts utilize and supervise the use of signals collection systems to identify, collect, and monitor foreign communications and geolocate targets; gist, transcribe, translate, analyze, summarize, and provide Quality Assurance (QA) on target foreign language communications; supervise collection management operations; coordinate collection, analysis, processing, exploitation, and reporting of target foreign intelligence; analyze target communications infrastructure; advise leadership on regional and cultural factors that impact mission operations; draft, validate, and release Signals Intelligence (SIGINT) reports; maintain cryptologic databases; perform target development; and protect sensitive methods and sources.

DoD Relationship **O*NET Relationship**

Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Analysis	123200	Intelligence Analysts	33-3021.00	Protective Service

Skills	Abilities
Critical Thinking	*Information Ordering*
Judgment and Decision Making	*Deductive Reasoning*
Active Learning	*Inductive Reasoning*
Complex Problem Solving	*Problem Sensitivity*
Writing	*Written Expression*
Operations Analysis	*Memorization*
Coordination	*Speed of Closure*
Reading Comprehension	*Category Flexibility*
Quality Control Analysis	*Perceptual Speed*
Systems Analysis	*Oral Expression*

COLLECTION OPERATIONS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze signal fundamentals and radio wave theory
E4	CORE	Apply collection sources and techniques
E4	CORE	Assess collection gaps
E5	NON-CORE	Assist in Unmanned Systems (UxS) operations
E4	CORE	Detect collection anomalies
E5	CORE	Manage selector taskings
E4	CORE	Perform remote sensor operations
E6	CORE	Process collection requirements (i.e., Collection Requirement Number (CRN) development)
E6	CORE	Provide corrective actions for collection anomalies
E4	CORE	Report collection anomalies
E4	CORE	Submit selectors for tasking
E6	CORE	Supervise cryptologic missions

INTELLIGENCE DISSEMINATION AND REPORTING

Paygrade	Task Type	Task Statements
E4	CORE	Annotate special dissemination controls
E4	CORE	Brief intelligence information
E4	CORE	Collaborate with other analysts on end products

INTELLIGENCE DISSEMINATION AND REPORTING (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Communicate Critical Intelligence Communications (CRITIC) information
E6	CORE	Coordinate special dissemination controls
E6	CORE	Coordinate with foreign entities (e.g., intelligence agencies, law enforcement, government institutions, corporations, etc.)
E4	CORE	Distribute time-sensitive alerts
E5	CORE	Draft Critical Intelligence Communications (CRITIC) messages
E4	CORE	Draft Signals Intelligence (SIGINT) reports
E4	CORE	Draft time-sensitive reports
E5	NON-CORE	Maintain Common Operational Picture (COP)
E6	CORE	Manage Signals Intelligence (SIGINT) reporting
E4	CORE	Map information flow within the Intelligence Cycle
E5	CORE	Perform Quality Assurance (QA) of Signals Intelligence (SIGINT) reports
E4	CORE	Provide Indications and Warning (I&W)
E5	CORE	Provide input to operational intelligence products (e.g., threat assessments, briefings, intelligence studies, etc.)
E4	CORE	Provide input to Requests for Information (RFI) responses
E4	CORE	Report Essential Elements of Information (EEI)
E4	CORE	Report potential threats
E7	CORE	Supervise Critical Intelligence Communications (CRITIC) reporting programs
E6	CORE	Validate Critical Intelligence Communications (CRITIC) messages

LANGUAGE ANALYSIS AND PROCESSING

Paygrade	Task Type	Task Statements
E4	CORE	Analyze content
E4	CORE	Articulate fundamental concepts related to Human Language Technologies (HLT)
E5	CORE	Assess regional and cultural factors that impact mission operations
E5	CORE	Conduct intelligence analysis within Target Office of Primary Interest (TOPI)
E4	CORE	Determine regional and cultural factors that impact mission operations
E4	CORE	Determine reporting criteria (e.g., geopolitical relevance, strategic relevance, anomalous activity, threat levels, etc.)
E5	NON-CORE	Develop language instructional materials
E4	CORE	Employ language processing tools
E4	CORE	Evaluate Signals of Interest (SOI)
E5	CORE	Integrate Human Language Technology (HLT) into language analysis workflow
E5	CORE	Perform historical analysis to answer strategic priorities
E5	CORE	Perform Quality Assurance (QA) of Interagency Language Roundtable (ILR) Level 2 language products
E6	CORE	Perform Quality Assurance (QA) of Interagency Language Roundtable (ILR) Level 2+ language products
E7	CORE	Perform Quality Assurance (QA) of Interagency Language Roundtable (ILR) Level 3 language products
E5	CORE	Perform Quality Assurance (QA) of language-related content in reports
E5	CORE	Prioritize data for processing

LANGUAGE ANALYSIS AND PROCESSING (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Process Interagency Language Roundtable (ILR) Level 2 target language material
E5	CORE	Process Interagency Language Roundtable (ILR) Level 2+ target language material
E6	CORE	Process Interagency Language Roundtable (ILR) Level 3 target language material
E6	NON-CORE	Provide global language instruction
E6	CORE	Provide input to Battle Damage Assessments (BDA)
E4	CORE	Provide near real-time/real-time language analysis
E4	CORE	Provide technical language input to mission planning
E6	CORE	Provide technical language instruction
E4	CORE	Report non-target languages or dialects
E4	CORE	Select software-based analysis tools

SECURITY AND ADMINISTRATION

Paygrade	Task Type	Task Statements
E4	CORE	Analyze roles, relationships, and responsibilities of elements of the Intelligence Community (IC)
E4	CORE	Apply Information Assurance (IA) fundamentals (i.e., confidentiality, integrity, availability, authentication, non-repudiation)
E4	CORE	Apply Information Security (INFOSEC) fundamentals (i.e., classifying and safeguarding classified National security information)
E4	CORE	Apply Intelligence Oversight (IO) fundamentals (e.g., protection of United States (U.S.) persons, Executive Order 12333, reporting, training, etc.)
E4	CORE	Apply provisions of the Foreign Intelligence Surveillance Act (FISA)
E4	CORE	Apply provisions of the United States Signals Intelligence Directives (USSID)
E6	CORE	Audit logical queries (e.g., Boolean, structured, etc.)
E6	CORE	Conduct cryptologic training exercises
E4	CORE	Control access to restricted areas
E6	CORE	Coordinate cryptologic missions
E5	CORE	Coordinate language skill maintenance
E4	CORE	Determine relevant information about the United States Signals Intelligence (SIGINT) System (USSS)
E7	CORE	Direct resources to meet mission requirements
E7	NON-CORE	Draft cryptologic operational policies and procedures
E7	CORE	Implement Emergency Destruction Plan (EDP)
E6	NON-CORE	Instruct courses within National Cryptologic University (NCU)
E6	NON-CORE	Manage Intelligence Oversight (IO)
E6	NON-CORE	Manage language training requirements
E7	CORE	Manage national cryptologic missions
E7	CORE	Manage operational assessment programs
E4	CORE	Perform pre-targeting compliance checks
E4	CORE	Protect Sensitive Compartmented Information (SCI) material
E5	CORE	Submit incident reports
E4	CORE	Transport Sensitive Compartmented Information (SCI) material

TARGET DEVELOPMENT AND EXPLOITATION

Paygrade	Task Type	Task Statements
E4	CORE	Access target technical information (e.g., technical kits, databases, working aids, etc.)
E5	NON-CORE	Analyze Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, Reconnaissance, and Target (C5ISRT) networks for critical nodes
E4	CORE	Analyze communication networks
E4	CORE	Analyze communication systems characteristics
E4	CORE	Analyze metadata
E5	CORE	Analyze target critical capabilities and vulnerabilities
E5	CORE	Analyze target tactics and methodologies (i.e., Tactics, Techniques, and Procedures (TTP))
E5	CORE	Analyze target threat capabilities
E4	CORE	Apply target tactics and methodologies (e.g., Tactics, Techniques, and Procedures (TTP), etc.)
E5	CORE	Assess computer network exploitation opportunities
E6	NON-CORE	Assess effectiveness of analysis tools
E5	NON-CORE	Assess effects of Operations in the Information Environment (OIE)
E4	NON-CORE	Assess situational data from Common Operational Picture (COP)
E4	CORE	Collaborate with other analysts on technical information
E5	CORE	Conduct Intelligence Preparation of the Operational Environment (IPOE)
E4	CORE	Construct logical queries (e.g., Boolean, structured, etc.)
E4	CORE	Determine communication network topography (e.g., hierarchy, base station, out station, etc.)
E4	CORE	Determine communication systems characteristics
E4	CORE	Determine digital network communications characteristics
E6	CORE	Determine intelligence gaps
E4	CORE	Determine location using geographic coordinates (e.g., Military Grid Reference System (MGRS), World Geographic Reference (GEOREF), etc.)
E5	CORE	Determine regional and cultural factors that influence target development
E4	CORE	Determine target capabilities
E4	CORE	Determine target location (e.g., geolocation, Direction Finding (DF), etc.)
E4	CORE	Determine telephony characteristics
E6	NON-CORE	Develop target packages (e.g., kinetic strikes, cyber effects, etc.)
E5	CORE	Develop target profiles
E5	CORE	Develop target technical information (e.g., technical kits, databases, working aids, etc.)
E5	NON-CORE	Draft Requests for Information (RFI)
E4	CORE	Evaluate target data using software-based analysis tools

TARGET DEVELOPMENT AND EXPLOITATION (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Implement principles of Signals Intelligence (SIGINT) Development (SIGDEV)
E6	NON-CORE	Integrate targeting efforts with other organizations and combatant commands
E4	CORE	Maintain target profiles
E5	CORE	Maintain technical databases
E4	CORE	Map communication networks
E5	CORE	Perform all-source research
E5	CORE	Perform digital network analysis
E5	CORE	Perform fusion analysis
E5	CORE	Perform Signals Intelligence (SIGINT) Development (SIGDEV)
E4	NON-CORE	Perform Signals Intelligence (SIGINT) Geospatial Analysis (SGA)
E5	CORE	Perform target development
E5	CORE	Perform trend/Pattern of Life (POL) analysis
E5	CORE	Provide input to battlespace environment evaluations
E6	NON-CORE	Provide input to Intelligence Gain/Loss (IGL) assessments
E5	NON-CORE	Provide input to Signals Intelligence (SIGINT) support packages
E4	CORE	Provide intelligence support to operations
E5	NON-CORE	Provide target nomination recommendations
E6	CORE	Supervise digital network analysis
E6	CORE	Supervise national cryptologic missions
E6	CORE	Supervise target activity analysis
E4	CORE	Update technical databases
E5	CORE	Validate intelligence sources
E7	NON-CORE	Validate Signals Intelligence (SIGINT) support packages

Job Title **Job Code**

Tactical Language Operator 001027

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Protective Service	TBD	TACTICAL LANGUAGE OPERATOR	TAC LANG OPR

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	CTI	NEC CXXX and 7XXX series and other NECs as assigned

Job Description

Tactical Language Operators utilize and supervise the use of signals collection equipment and systems to provide Indications and Warning (I&W) support to Fleet and Combatant Commanders; collect, analyze, identify and geolocate target communications and infrastructure; gist, translate, transcribe, summarize and report on target foreign language communications in real-time; provide Quality Assurance (QA) on information products; advise leadership on regional and cultural factors that impact mission operations; perform target development; and protect sensitive methods and sources.

DoD Relationship **O*NET Relationship**

Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Analysis	123200	Intelligence Analysts	33-3021.00	Protective Service

Skills	Abilities
Critical Thinking	*Information Ordering*
Judgment and Decision Making	*Deductive Reasoning*
Active Learning	*Inductive Reasoning*
Operations Analysis	*Problem Sensitivity*
Writing	*Written Expression*
Complex Problem Solving	*Speed of Closure*
Coordination	*Category Flexibility*
Quality Control Analysis	*Memorization*
Reading Comprehension	*Oral Expression*
Systems Analysis	*Perceptual Speed*

COLLECTION OPERATIONS

Paygrade	Task Type	Task Statements
E7	NON-CORE	Adjust collection plans (e.g., Direct Support Element (DSE) supervisor, Tactical Information Operations (TIO) Analyst, etc.)
E6	CORE	Advise platform commanders on Courses of Action (COA)
E4	CORE	Analyze signal fundamentals and radio wave theory
E4	CORE	Apply collection sources and techniques
E4	CORE	Assess collection gaps
E5	NON-CORE	Assist in Unmanned Systems (UxS) operations
E6	CORE	Conduct pre-operational checks of organic collection equipment
E4	CORE	Configure collection systems (e.g., Radio Frequency (RF), metadata, etc.)
E7	CORE	Construct technical mission plans compatible with onboard collection systems
E5	CORE	Coordinate target location operations (e.g., geolocation, Direction Finding (DF), etc.)
E6	CORE	Deliver organic collection data from platform to United States Signals Intelligence (SIGINT) System (USSS)
E4	CORE	Detect collection anomalies
E4	CORE	Initialize collection systems
E7	CORE	Manage Distributed Signals Intelligence (SIGINT) Operations (DSO)
E5	CORE	Manage selector taskings
E5	CORE	Operate platform-specific collection equipment

COLLECTION OPERATIONS (CONT'D)

Paygrade	Task Type	Task Statements
E5	CORE	Optimize collection systems
E4	CORE	Perform Distributed Signals Intelligence (SIGINT) Operations (DSO)
E4	CORE	Perform remote sensor operations
E5	CORE	Perform survey operations
E6	CORE	Process collection requirements (i.e., Collection Requirement Number (CRN) development)
E6	CORE	Provide corrective actions for collection anomalies
E6	CORE	Provide input to Cryptologic Coverage Plans (CCP)
E6	CORE	Recommend platform disposition to optimize Signals Intelligence (SIGINT) collection
E4	CORE	Report collection anomalies
E4	CORE	Submit selectors for tasking
E6	CORE	Supervise cryptologic missions
E6	CORE	Troubleshoot organic collection equipment
E7	CORE	Validate Collection Management Authority (CMA) requirements

INTELLIGENCE DISSEMINATION AND REPORTING

Paygrade	Task Type	Task Statements
E4	CORE	Annotate special dissemination controls
E4	CORE	Brief intelligence information
E4	CORE	Collaborate with other analysts on end products
E4	CORE	Communicate Critical Intelligence Communications (CRITIC) information
E6	CORE	Coordinate special dissemination controls
E6	CORE	Coordinate with foreign entities (e.g., intelligence agencies, law enforcement, government institutions, corporations, etc.)
E4	CORE	Distribute time-sensitive alerts
E5	CORE	Draft Critical Intelligence Communications (CRITIC) messages
E5	NON-CORE	Draft post-mission products
E4	CORE	Draft Signals Intelligence (SIGINT) reports
E4	CORE	Draft time-sensitive reports
E5	NON-CORE	Maintain Common Operational Picture (COP)
E6	CORE	Manage Signals Intelligence (SIGINT) reporting
E4	CORE	Map information flow within the Intelligence Cycle
E5	CORE	Perform Quality Assurance (QA) of Signals Intelligence (SIGINT) reports
E4	CORE	Provide Indications and Warning (I&W)
E5	CORE	Provide input to operational intelligence products (e.g., threat assessments, briefings, intelligence studies, etc.)
E4	CORE	Provide input to Requests for Information (RFI) responses
E4	CORE	Report Essential Elements of Information (EEI)
E4	CORE	Report potential threats
E6	NON-CORE	Submit priority recommendations to support Commanders Critical Information Requirements (CCIR)
E7	CORE	Supervise Critical Intelligence Communications (CRITIC) reporting programs

INTELLIGENCE DISSEMINATION AND REPORTING (CONT'D)

Paygrade	Task Type	Task Statements
E6	CORE	Validate Critical Intelligence Communications (CRITIC) messages

LANGUAGE ANALYSIS AND PROCESSING

Paygrade	Task Type	Task Statements
E4	CORE	Analyze content
E4	CORE	Articulate fundamental concepts related to Human Language Technologies (HLT)
E5	CORE	Assess regional and cultural factors that impact mission operations
E4	CORE	Determine regional and cultural factors that impact mission operations
E4	CORE	Determine reporting criteria (e.g., geopolitical relevance, strategic relevance, anomalous activity, threat levels, etc.)
E5	NON-CORE	Develop language instructional materials
E4	CORE	Employ language processing tools
E4	CORE	Evaluate Signals of Interest (SOI)
E5	CORE	Integrate Human Language Technology (HLT) into language analysis workflow
E5	CORE	Perform Quality Assurance (QA) of Interagency Language Roundtable (ILR) Level 2 language products
E6	CORE	Perform Quality Assurance (QA) of Interagency Language Roundtable (ILR) Level 2+ language products
E7	CORE	Perform Quality Assurance (QA) of Interagency Language Roundtable (ILR) Level 3 language products
E5	CORE	Perform Quality Assurance (QA) of language-related content in reports
E5	CORE	Prioritize data for processing
E4	CORE	Process Interagency Language Roundtable (ILR) Level 2 target language material
E5	CORE	Process Interagency Language Roundtable (ILR) Level 2+ target language material
E6	CORE	Process Interagency Language Roundtable (ILR) Level 3 target language material
E6	NON-CORE	Provide global language instruction
E6	CORE	Provide input to Battle Damage Assessments (BDA)
E4	CORE	Provide near real-time/real-time language analysis
E4	CORE	Provide technical language input to mission planning
E6	CORE	Provide technical language instruction
E4	CORE	Report non-target languages or dialects
E4	CORE	Select software-based analysis tools

SECURITY AND ADMINISTRATION

Paygrade	Task Type	Task Statements
E4	CORE	Analyze roles, relationships, and responsibilities of elements of the Intelligence Community (IC)
E4	CORE	Apply Information Assurance (IA) fundamentals (i.e., confidentiality, integrity, availability, authentication, non-repudiation)
E4	CORE	Apply Information Security (INFOSEC) fundamentals (i.e., classifying and safeguarding classified National security information)
E4	CORE	Apply Intelligence Oversight (IO) fundamentals (e.g., protection of United States (U.S.) persons, Executive Order 12333, reporting, training, etc.)
E4	CORE	Apply provisions of the Foreign Intelligence Surveillance Act (FISA)

SECURITY AND ADMINISTRATION (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Apply provisions of the United States Signals Intelligence Directives (USSID)
E6	CORE	Audit logical queries (e.g., Boolean, structured, etc.)
E6	CORE	Conduct cryptologic training exercises
E4	CORE	Control access to restricted areas
E7	CORE	Coordinate augmentation teams for deployment support
E6	CORE	Coordinate cryptologic missions
E5	CORE	Coordinate language skill maintenance
E4	CORE	Determine relevant information about the United States Signals Intelligence (SIGINT) System (USSS)
E7	CORE	Direct resources to meet mission requirements
E7	NON-CORE	Draft cryptologic operational policies and procedures
E7	CORE	Implement Emergency Destruction Plan (EDP)
E6	NON-CORE	Manage Intelligence Oversight (IO)
E6	NON-CORE	Manage language training requirements
E7	CORE	Manage operational assessment programs
E4	CORE	Perform pre-targeting compliance checks
E4	CORE	Protect Sensitive Compartmented Information (SCI) material
E5	CORE	Submit incident reports
E4	CORE	Transport Sensitive Compartmented Information (SCI) material

TARGET DEVELOPMENT AND EXPLOITATION

Paygrade	Task Type	Task Statements
E4	CORE	Access target technical information (e.g., technical kits, databases, working aids, etc.)
E5	NON-CORE	Analyze Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, Reconnaissance, and Target (C5ISRT) networks for critical nodes
E4	CORE	Analyze communication networks
E4	CORE	Analyze communication systems characteristics
E4	CORE	Analyze metadata
E5	CORE	Analyze target critical capabilities and vulnerabilities
E5	CORE	Analyze target tactics and methodologies (i.e., Tactics, Techniques, and Procedures (TTP))
E5	CORE	Analyze target threat capabilities
E4	CORE	Apply target tactics and methodologies (e.g., Tactics, Techniques, and Procedures (TTP), etc.)
E6	NON-CORE	Assess effectiveness of analysis tools
E5	NON-CORE	Assess effects of Operations in the Information Environment (OIE)
E4	NON-CORE	Assess situational data from Common Operational Picture (COP)
E4	CORE	Collaborate with other analysts on technical information
E5	CORE	Conduct Intelligence Preparation of the Operational Environment (IPOE)
E4	CORE	Construct logical queries (e.g., Boolean, structured, etc.)

TARGET DEVELOPMENT AND EXPLOITATION (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Determine communication network topography (e.g., hierarchy, base station, out station, etc.)
E4	CORE	Determine communication systems characteristics
E4	CORE	Determine digital network communications characteristics
E6	CORE	Determine intelligence gaps
E4	CORE	Determine location using geographic coordinates (e.g., Military Grid Reference System (MGRS), World Geographic Reference (GEOREF), etc.)
E5	CORE	Determine regional and cultural factors that influence target development
E4	CORE	Determine target capabilities
E4	CORE	Determine target location (e.g., geolocation, Direction Finding (DF), etc.)
E4	CORE	Determine telephony characteristics
E6	NON-CORE	Develop target packages (e.g., kinetic strikes, cyber effects, etc.)
E5	CORE	Develop target profiles
E5	CORE	Develop target technical information (e.g., technical kits, databases, working aids, etc.)
E5	NON-CORE	Draft Requests for Information (RFI)
E4	CORE	Evaluate target data using software-based analysis tools
E4	CORE	Implement principles of Signals Intelligence (SIGINT) Development (SIGDEV)
E6	NON-CORE	Integrate targeting efforts with other organizations and combatant commands
E4	CORE	Maintain target profiles
E5	CORE	Maintain technical databases
E4	CORE	Map communication networks
E5	CORE	Perform all-source research
E5	CORE	Perform fusion analysis
E5	CORE	Perform Signals Intelligence (SIGINT) Development (SIGDEV)
E4	NON-CORE	Perform Signals Intelligence (SIGINT) Geospatial Analysis (SGA)
E5	CORE	Perform target development
E5	CORE	Perform trend/Pattern of Life (POL) analysis
E5	CORE	Provide input to battlespace environment evaluations
E6	NON-CORE	Provide input to Intelligence Gain/Loss (IGL) assessments
E5	NON-CORE	Provide input to Signals Intelligence (SIGINT) support packages
E4	CORE	Provide intelligence support to operations
E5	NON-CORE	Provide target nomination recommendations
E6	CORE	Supervise target activity analysis
E5	NON-CORE	Support remote access operations
E4	CORE	Update technical databases
E5	CORE	Validate intelligence sources
E7	NON-CORE	Validate Signals Intelligence (SIGINT) support packages
E7	NON-CORE	Validate target packages (e.g., kinetic strikes, cyber effects, etc.)

Job Title **Job Code**

Cyber Language Analyst 002683

Job Family	NOC	Short Title (30 Characters)	Short Title (14 Characters)
Protective Service	TBD	CYBER LANGUAGE ANALYST	CYB LANG ANLST

Pay Plan	Career Field	Other Relationships and Rules
Enlisted	CTI	NEC CXXX and 7XXX series and other NECs as assigned

Job Description

Cyber Language Analysts conduct and supervise language analysis in support of offensive and defensive cyberspace operations to meet National, Joint, Fleet, and Combatant Commander requirements; gist, transcribe, translate, summarize, analyze, and report foreign language communications and digital network information to support exploitation of target networks and critical infrastructure; provide Quality Assurance (QA) on intelligence products; perform cyberspace target development, exploitation analysis, network mapping, forensic analysis, and discovery; advise leadership on regional and cultural factors that impact cyberspace operations; and protect sensitive methods and sources.

DoD Relationship		O*NET Relationship		
Group Title	*DoD Code*	*Occupation Title*	*SOC Code*	*Job Family*
Analysis	123200	Intelligence Analysts	33-3021.06	Protective Service

Skills	Abilities
Critical Thinking	*Information Ordering*
Judgment and Decision Making	*Deductive Reasoning*
Active Learning	*Inductive Reasoning*
Operations Analysis	*Problem Sensitivity*
Writing	*Written Expression*
Complex Problem Solving	*Speed of Closure*
Coordination	*Category Flexibility*
Quality Control Analysis	*Memorization*
Reading Comprehension	*Oral Expression*
Systems Analysis	*Perceptual Speed*

COLLECTION OPERATIONS

Paygrade	Task Type	Task Statements
E4	CORE	Analyze signal fundamentals and radio wave theory
E4	CORE	Apply collection sources and techniques
E5	CORE	Assess collection gaps
E4	CORE	Detect collection anomalies
E5	CORE	Manage selector taskings
E5	CORE	Perform survey operations
E6	CORE	Process collection requirements (i.e., Collection Requirement Number (CRN) development)
E6	CORE	Provide corrective actions for collection anomalies
E4	CORE	Report collection anomalies
E4	CORE	Submit selectors for tasking

INTELLIGENCE DISSEMINATION AND REPORTING

Paygrade	Task Type	Task Statements
E4	CORE	Annotate special dissemination controls
E4	CORE	Brief intelligence information
E4	CORE	Collaborate with other analysts on end products
E4	CORE	Communicate Critical Intelligence Communications (CRITIC) information
E6	CORE	Coordinate special dissemination controls

INTELLIGENCE DISSEMINATION AND REPORTING (CONT'D)

Paygrade	Task Type	Task Statements
E6	CORE	Coordinate with foreign entities (e.g., intelligence agencies, law enforcement, government institutions, corporations, etc.)
E5	CORE	Draft Critical Intelligence Communications (CRITIC) messages
E5	NON-CORE	Draft post-mission products
E4	CORE	Draft Signals Intelligence (SIGINT) reports
E6	CORE	Manage Signals Intelligence (SIGINT) reporting
E4	CORE	Map information flow within the Intelligence Cycle
E5	CORE	Perform Quality Assurance (QA) of Signals Intelligence (SIGINT) reports
E6	CORE	Provide input into cyberspace operations reporting
E5	CORE	Provide input to operational intelligence products (e.g., threat assessments, briefings, intelligence studies, etc.)
E4	CORE	Provide input to Requests for Information (RFI) responses
E4	CORE	Report Essential Elements of Information (EEI)
E4	CORE	Report potential threats
E6	NON-CORE	Submit priority recommendations to support Commanders Critical Information Requirements (CCIR)
E7	CORE	Supervise Critical Intelligence Communications (CRITIC) reporting programs
E6	CORE	Validate Critical Intelligence Communications (CRITIC) messages

LANGUAGE ANALYSIS AND PROCESSING

Paygrade	Task Type	Task Statements
E5	CORE	Advise on cyber adversary defense posture
E4	CORE	Analyze content
E4	CORE	Articulate fundamental concepts related to Human Language Technologies (HLT)
E5	CORE	Assess regional and cultural factors that impact mission operations
E4	CORE	Determine regional and cultural factors that impact mission operations
E4	CORE	Determine reporting criteria (e.g., geopolitical relevance, strategic relevance, anomalous activity, threat levels, etc.)
E5	NON-CORE	Develop language instructional materials
E4	CORE	Employ language processing tools
E4	CORE	Evaluate Signals of Interest (SOI)
E5	CORE	Integrate Human Language Technology (HLT) into language analysis workflow
E5	CORE	Perform Quality Assurance (QA) of Interagency Language Roundtable (ILR) Level 2 language products
E6	CORE	Perform Quality Assurance (QA) of Interagency Language Roundtable (ILR) Level 2+ language products
E7	CORE	Perform Quality Assurance (QA) of Interagency Language Roundtable (ILR) Level 3 language products
E5	CORE	Perform Quality Assurance (QA) of language-related content in reports
E5	CORE	Prioritize data for processing
E4	CORE	Process Interagency Language Roundtable (ILR) Level 2 target language material
E5	CORE	Process Interagency Language Roundtable (ILR) Level 2+ target language material
E6	CORE	Process Interagency Language Roundtable (ILR) Level 3 target language material

LANGUAGE ANALYSIS AND PROCESSING (CONT'D)

Paygrade	Task Type	Task Statements
E6	NON-CORE	Provide global language instruction
E6	CORE	Provide input to Battle Damage Assessments (BDA)
E4	CORE	Provide near real-time/real-time language analysis
E4	CORE	Provide technical language input to mission planning
E6	CORE	Provide technical language instruction
E4	CORE	Report non-target languages or dialects
E4	CORE	Select software-based analysis tools
E6	CORE	Validate cyber adversary defense posture

SECURITY AND ADMINISTRATION

Paygrade	Task Type	Task Statements
E4	CORE	Analyze roles, relationships, and responsibilities of elements of the Intelligence Community (IC)
E4	CORE	Apply Information Assurance (IA) fundamentals (i.e., confidentiality, integrity, availability, authentication, non-repudiation)
E4	CORE	Apply Information Security (INFOSEC) fundamentals (i.e., classifying and safeguarding classified National security information)
E4	CORE	Apply Intelligence Oversight (IO) fundamentals (e.g., protection of United States (U.S.) persons, Executive Order 12333, reporting, training, etc.)
E4	CORE	Apply provisions of the Foreign Intelligence Surveillance Act (FISA)
E4	CORE	Apply provisions of the United States Signals Intelligence Directives (USSID)
E6	CORE	Audit logical queries (e.g., Boolean, structured, etc.)
E6	CORE	Conduct cryptologic training exercises
E4	CORE	Control access to restricted areas
E6	CORE	Coordinate cryptologic missions
E5	CORE	Coordinate language skill maintenance
E4	CORE	Determine relevant information about the United States Signals Intelligence (SIGINT) System (USSS)
E7	CORE	Direct resources to meet mission requirements
E7	NON-CORE	Draft cyberspace operations policies and procedures
E7	NON-CORE	Draft policies and procedures in support of cyberspace operations
E7	CORE	Implement Emergency Destruction Plan (EDP)
E6	NON-CORE	Manage Intelligence Oversight (IO)
E6	NON-CORE	Manage language training requirements
E7	CORE	Manage operational assessment programs
E4	CORE	Perform pre-targeting compliance checks
E4	CORE	Protect Sensitive Compartmented Information (SCI) material
E5	CORE	Submit incident reports
E4	CORE	Transport Sensitive Compartmented Information (SCI) material

TARGET DEVELOPMENT AND EXPLOITATION

Paygrade	Task Type	Task Statements
E4	CORE	Access target technical information (e.g., technical kits, databases, working aids, etc.)
E5	NON-CORE	Analyze Command, Control, Communications, Computers, Combat Systems, Intelligence, Surveillance, Reconnaissance, and Target (C5ISRT) networks for critical nodes
E4	CORE	Analyze communication networks
E4	CORE	Analyze communication systems characteristics
E4	CORE	Analyze metadata
E5	CORE	Analyze target critical capabilities and vulnerabilities
E5	CORE	Analyze target tactics and methodologies (i.e., Tactics, Techniques, and Procedures (TTP))
E5	CORE	Analyze target threat capabilities
E4	CORE	Apply target tactics and methodologies (e.g., Tactics, Techniques, and Procedures (TTP), etc.)
E5	CORE	Assess computer network exploitation opportunities
E6	NON-CORE	Assess effectiveness of analysis tools
E5	NON-CORE	Assess effects of Operations in the Information Environment (OIE)
E4	CORE	Collaborate with other analysts on technical information
E5	CORE	Conduct Intelligence Preparation of the Operational Environment (IPOE)
E4	CORE	Construct logical queries (e.g., Boolean, structured, etc.)
E5	CORE	Coordinate cyberspace missions
E6	CORE	Coordinate exploitation of access vectors for networks of interest
E6	NON-CORE	Determine capabilities of cyber assets relevant to specific target area
E4	CORE	Determine communication network topography (e.g., hierarchy, base station, out station, etc.)
E4	CORE	Determine communication systems characteristics
E4	CORE	Determine digital network communications characteristics
E6	CORE	Determine intelligence gaps
E4	CORE	Determine location using geographic coordinates (e.g., Military Grid Reference System (MGRS), World Geographic Reference (GEOREF), etc.)
E5	CORE	Determine regional and cultural factors that influence target development
E5	NON-CORE	Determine software and hardware vulnerabilities
E4	CORE	Determine target capabilities
E4	CORE	Determine target location (e.g., geolocation, Direction Finding (DF), etc.)
E4	CORE	Determine telephony characteristics
E6	NON-CORE	Develop target packages (e.g., kinetic strikes, cyber effects, etc.)
E5	CORE	Develop target profiles
E5	CORE	Develop target technical information (e.g., technical kits, databases, working aids, etc.)
E5	NON-CORE	Draft Requests for Information (RFI)
E5	CORE	Enable cyberspace exploitation operations
E4	CORE	Evaluate target data using software-based analysis tools

TARGET DEVELOPMENT AND EXPLOITATION (CONT'D)

Paygrade	Task Type	Task Statements
E4	CORE	Implement principles of Signals Intelligence (SIGINT) Development (SIGDEV)
E6	CORE	Initialize cyberspace exploitation operations
E6	NON-CORE	Integrate targeting efforts with other organizations and combatant commands
E4	CORE	Maintain target profiles
E5	CORE	Maintain technical databases
E4	CORE	Map communication networks
E5	CORE	Perform all-source research
E5	CORE	Perform digital network analysis
E5	CORE	Perform fusion analysis
E5	CORE	Perform logical network analysis
E5	CORE	Perform Signals Intelligence (SIGINT) Development (SIGDEV)
E4	NON-CORE	Perform Signals Intelligence (SIGINT) Geospatial Analysis (SGA)
E5	CORE	Perform target development
E5	CORE	Perform trend/Pattern of Life (POL) analysis
E6	CORE	Produce reconstruction of logical networks
E6	NON-CORE	Provide input to Intelligence Gain/Loss (IGL) assessments
E5	NON-CORE	Provide input to Signals Intelligence (SIGINT) support packages
E4	CORE	Provide intelligence support to operations
E5	NON-CORE	Provide target nomination recommendations
E6	NON-CORE	Supervise cyberspace missions
E6	CORE	Supervise digital network analysis
E6	CORE	Supervise logical network analysis
E6	CORE	Supervise target activity analysis
E5	NON-CORE	Support remote access operations
E4	CORE	Update technical databases
E5	CORE	Validate intelligence sources
E7	NON-CORE	Validate target packages (e.g., kinetic strikes, cyber effects, etc.)