Appendix B Removed

MCRP 2-10A.1

Signals Intelligence

U.S. Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 144 000237 01

UNITED STATES MARINE CORPS

12 April 2022

FOREWORD

Marine Corps Reference Publication (MCRP) 2-10A.1, *Signals Intelligence*, serves as a basic reference for understanding concepts, operations, and procedures for the conduct of signals intelligence (SIGINT) operations in support of the Marine air-ground task force. This publication complements and expands on Marine Corps Doctrinal Publication 2, *Intelligence*, and Marine Corps Warfighting Publication 2-10, *Intelligence Operations*, which provide doctrine and higher order tactics, techniques, and procedures for intelligence operations.

The primary target audience of this publication is intelligence personnel responsible for planning and executing SIGINT operations. Personnel who provide support to SIGINT or who use the results from these operations should also read this publication. MCRP 2-10A.1 describes aspects of SIGINT operations, including doctrinal fundamentals, equipment, command and control, communications and information systems support, planning, execution, security, and training. Detailed information on SIGINT operations and tactics, techniques, and procedures is classified and beyond the scope of this publication.

This publication supersedes MCWP 2-15.2, *Signals Intelligence*, dated 22 February 1999, MCWP 2-22, *Signals Intelligence*, dated 13 July 2004, MCRP 2-10A, *Signals Intelligence*, 1 dated 2 May 2016, and change 1 dated 4 April 2018.

Reviewed and approved this date.

SETH E. ANDERSON
Colonel, U.S. Marine Corps
Commanding Officer, Marine Corps Intelligence School

Publication Control Number: 144 000237 01

Table of Contents

Chapter 1. Signals Intelligence Operating Environment

Chapter 2. Signals Intelligence

Chapter 3. Signals Intelligence Authorities, Oversight, Tasking, and Control

Chapter 4.
Signals Intelligence Community

Chapter 5. Signals Intelligence Communications Architecture

Chapter 6. Planning and Operations

Appendices

Glossary Section I. Abbreviations and Acronyms

Glossary Section II. Terms and Definitions

References and Related Publications

Copyright Information

CHAPTER 1. SIGNALS INTELLIGENCE OPERATING ENVIRONMENT

Signals intelligence (SIGINT) is a discipline within the field of intelligence that derives intelligence from information and data signals—whether wired or wireless. Understanding radio frequency, network, and communications theories are necessary skills used to conduct SIGINT in an electromagnetic operating environment (EMOE). This chapter outlines the diversity and complexity of the signals environment faced by the United States Signals Intelligence System (USSS), which includes Marine Corps SIGINT.

INTELLIGENCE AND INTELLIGENCE OPERATIONS

Intelligence

DOD Dictionary of Military and Associated Terms defines intelligence as:

> The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity.

Intelligence is one of the seven warfighting functions. It helps commanders understand the enemy and the battlespace by providing information about the situation, alerting them to new opportunities, and helping them assess an action's impact on the enemy or the environment. Intelligence drives operations through operational requirements to support command and control (C2), fires, maneuver, force protection, and logistics. Commander's intent and priority intelligence requirements (PIRs) guide intelligence.

Intelligence is made of information, and this information is formed from data. Just as one or more pieces of data may create information, one or more pieces of information may create intelligence. The means by which information is converted into intelligence and made available to users is known as the intelligence process. Figure 1-1 depicts the relationship of data, information, and intelligence and shows correlations to intelligence process operations.

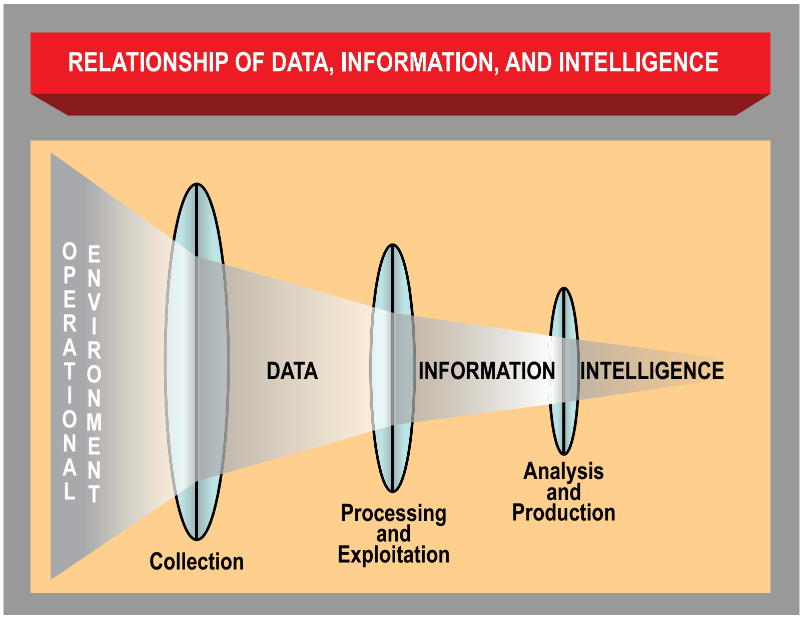


Figure 1-1. Relationship of Data, Information, and Intelligence.

Information is the meaning that humans assign to data using known conventions for representation. Data consists of raw representations of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing, either by human or automated means. Data also consists of representations, such as characters or analog quantities, to which meaning can be assigned. The intelligence process is used against data and/or information to provide a commander or customer with knowledge.

Intelligence Operations

Intelligence operations are wide-ranging activities conducted by intelligence staffs and organizations to provide commanders and national level decision makers with relevant, accurate, and timely intelligence. A command's intelligence operation is published in Annex B to the operations order. It describes how the six steps in the intelligence cycle/process are used to support the commander's decision making and overall mission success. The six steps in the intelligence cycle/process are:

- Planning and direction.
- Collection.
- Processing and exploitation.
- Analysis and production.
- Dissemination and integration.
- Evaluation and feedback.

Figure 1-2 shows the six categories of the intelligence process.

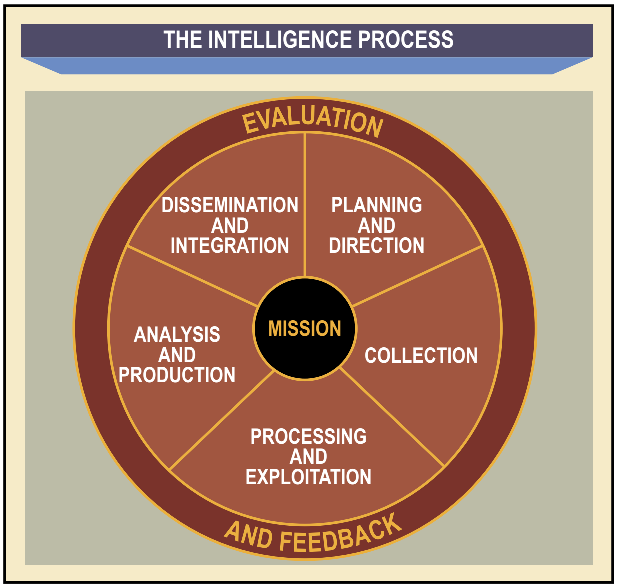
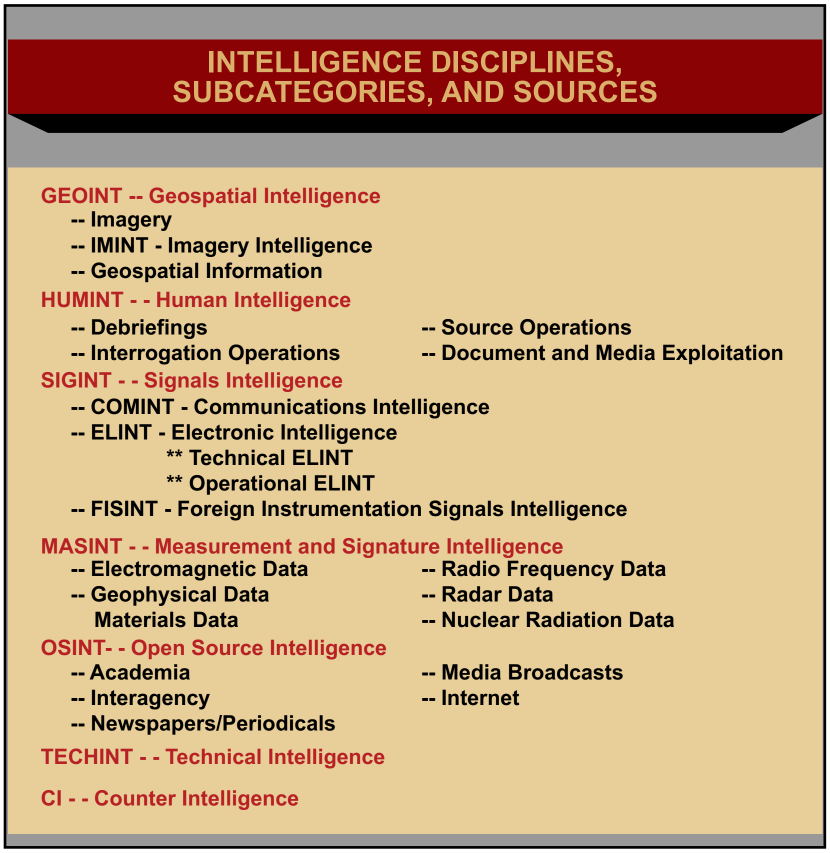


Figure 1-2. The intelligence Process.

Intelligence is subdivided into different disciplines. These disciplines have explicit laws and policies that govern them. Intelligence collection planning should consider ways to best leverage the strong points and minimize the weak points of each intelligence discipline. Intelligence disciplines are split into seven recognized areas:

- GEOINT (Geospatial intelligence).
- Human intelligence (HUMINT).
- SIGINT.
- Measurement and signature intelligence (MASINT).
- OSINT (Open source intelligence).
- Technical intelligence (TECHINT).
- Counterintelligence (CI).

As shown in figure 1-3, intelligence personnel use these disciplines in concert to complement and support analytic conclusions in an integrated, multi-disciplined approach to intelligence analysis.



INTELLIGENCE DISCIPLINES,
SUBCATEGORIES, AND SOURCES

GEOINT -- Geospatial Intelligence
-- Imagery
-- IMINT - Imagery Intelligence
-- Geospatial Information

HUMINT - - Human Intelligence
-- Debriefings
-- Interrogation Operations
-- Source Operations
-- Document and Media Exploitation

SIGINT - - Signals Intelligence
-- COMINT - Communications Intelligence
-- ELINT - Electronic Intelligence
** Technical ELINT
** Operational ELINT
-- FISINT - Foreign Instrumentation Signals Intelligence

MASINT - - Measurement and Signature Intelligence
-- Electromagnetic Data
-- Geophysical Data
Materials Data
-- Radio Frequency Data
-- Radar Data
-- Nuclear Radiation Data

OSINT- - Open Source Intelligence
-- Academia
-- Interagency
-- Newspapers/Periodicals
-- Media Broadcasts
-- Internet

TECHINT - - Technical Intelligence

CI - - Counter Intelligence

Figure 1-3. Intelligence Disciplines.

Signals Environment

The electromagnetic spectrum (EMS) ranges from 3 Hz to 300 EHz, but the portion of the EMS suitable for communications—the radio frequency (RF) domain—is narrower. The RF domain, where nearly all signals of interest (SOIs) reside, ranges from extremely low frequency at 3 Hz to extremely high frequency at 300 GHz.

An SOI is a signal within, or that relates to, the Marine Air Ground Task Force (MAGTF) area of interest (AOI) that when exploited provides the commander with information or intelligence. Adversaries of the United States use electronic signals for many functions, including command and control, intelligence, fire and maneuver coordination, target acquisition and tracking, and weapons guidance.

SIGNAL FUNDAMENTALS

Signals allow voice, images, video, text/data communications, or non communications data to be transmitted over long distances. The common term "communications" is technically known as telecommunications. Telecommunications include any transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems. Non communications are data signals that carry detection and ranging information such as radar or beaconing emissions. Signals Intelligence focuses on collecting and exploiting signals which contain information, regardless of format, and identifying the geospatial location from which the signal originated.

Worldwide development and use of emerging technologies and electronic devices are growing exponentially, and is increasing congestion and competition within the EMS and the EMOE. Congestion in the EMOE makes the signals environment more complex and difficult to prosecute SOIs. Historically, the development of military communications and non-communications technologies was isolated from commercial technologies. However, this isolation is rapidly eroding due to the commercial market and consumer desire for more and more EMS frequency space. The result of this spectrum crowding and reduced dedicated military bandwidth means that SIGINT has become an even harder job to perform. Further, asymmetric forces that lack robust and secure communications use new and emergent technologies to achieve nation-state-like capabilities to command, control, and communicate.

Signals Intelligence operational environments are not restricted to a geographic area or communication technology. A target may have access to multiple communication methods of that extend beyond the confines of the MAGTF battlespace geometry. To access information relevant to the MAGTF's mission, different signal collection strategies must be employed at various points along the target transmission path. Signals Intelligence requires MAGTF organic and non organic assets to work together to collect, process, analyze, and share relevant information. This national and tactical integration of SIGINT capability places more emphasis on necessary training and skill-set development required of Marine SIGINT personnel so they can support the commander and other decision makers.

CHAPTER 2.
SIGNALS INTELLIGENCE

SIGNALS INTELLIGENCE DEFINITION

Signals Intelligence is defined as "a category of intelligence comprising, either individually or in combination, all communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT), however transmitted." Put another way, SIGINT is the intelligence derived from communications, electronic, and/or foreign instrumentation signals. Due to the classification of SIGINT sources and methods, and the highly perishable nature of SIGINT capabilities, many details about SIGINT operations and tactics, techniques, and procedures (TTPs) cannot be provided in this document. Additional information on most subjects is located in the references.

Signals Intelligence applies the intelligence process against electromagnetic signals to gain undetected, first-hand intelligence on the adversary's activities, intentions, dispositions, capabilities, and limitations. Adversary networks and equipment may be arranged in a traditional method as seen in state-controlled armed forces (classic hierarchy e.g., centralized command and control an integrated air defense system) or in an irregular method as seen in non-state threat groups (decentralized cells, e.g., insurgent, criminal, or terror networks) that use communications. Signals Intelligence operations seek to exploit such network communications paths. Based on collecting and analyzing signals of interest, the ultimate end state for SIGINT operations is to deliver critical information obtained from targeted signals to decision makers and intelligence consumers at all levels. Fusion analysts will combine SIGINT products and reporting with other intelligence sources to better understand the environment.

The SIGINT operational environment focuses on signals that impact the MAGTF AOI but are not necessarily confined to geographic boundaries. Signals Intelligence operations are complex and multi-faceted, requiring integrating organic, theater, and national capabilities to deliver relevant intelligence to the MAGTF. The concept of National to tactical integration (NTI) has proven its value supporting Marine Corps operations since its inception in 1995. Future SIGINT operations supporting MAGTF intelligence and operations will continue to rely on NTI.

SIGNALS INTELLIGENCE PURPOSE

The purpose of Marine Corps tactical SIGINT is to support the commander and other decision makers with intelligence derived from processed electromagnetic signals, and "reachback" capabilities from the MAGTF to national USSS and partner SIGINT organizations.

Signals Intelligence adds intelligence value regarding the adversary's current and future actions, intentions, and locations across the range of military operations. It also amplifies understanding of the AO through non adversarial collection that provides atmospherics (non adversarial intentions, actions, relationships, locations, and other information that affects security, governance, and economics).

SIGNALS INTELLIGENCE DISCIPLINES

Signals Intelligence is separated into the following three sub-disciplines:

Communications Intelligence

Communications Intelligence is the technical and intelligence information derived from foreign communications by anyone other than the intended recipient. Technical information describes characteristics, procedures, or equipment directly related to communications or the analysis of communications.

Electronic Intelligence

Electronic Intelligence has two subcategories and is derived from interception and analysis of non-communications emitters, including radar:

- Operational electronic intelligence (OPELINT).
- Technical electronic intelligence (TECHELINT).

Operational Electronic Intelligence. Operational Electronic Intelligence is operationally relevant information such as the location, movement, employment, tactics, and activity of foreign non communications emitters and their associated weapon systems.

Technical Electronic Intelligence. Technical Electronic Intelligence refers to the technical aspects of foreign non communications emitters, such as performance parameters, signal characteristics, modes, functions, associations, capabilities, limitations, vulnerabilities, and technology levels. TECHELINT is primarily strategic in nature, yet the future EMOE will require some level of TECHELINT to be performed at the tactical edge of operations.

Foreign Instrumentation Signals Intelligence

Foreign Instrumentation Signals Intelligence is the technical analysis of data intercepted from foreign equipment and control systems, such as:

- Telemetry.
- Electronic interrogators.
- Command system tracking, fusing, arming, and firing.
- Video data links.

Foreign Instrumentation Signals Intelligence is primarily strategic in nature.

SIGNALS INTELLIGENCE PROCESS

The SIGINT process mirrors and feeds the intelligence process. Accordingly, the SIGINT process includes the following six phases:

- Planning and direction.
- Collection.
- Processing and exploitation.
- Analysis and production.
- Dissemination and integration.
- Evaluation and feedback.

The SIGINT community conducts a wide range of tasks within each phase of the SIGINT process.

Signals Intelligence Planning and Direction

For information related to SIGINT planning and direction, refer to chapter 6, Planning and Operations.

Signals Intelligence Collection, Processing, and Exploitation

The collection, processing, and exploitation phases are usually conducted together, although advanced processing and exploitation may be conducted from separate locations.

Signals Intelligence collection is the acquisition of a signal and the provision of this information to processing elements. The output is a collected SOI.

During SIGINT processing, an SOI is converted to usable data. Processing includes demodulation, decryption (if possible), and/or converting data (i.e., digital or analog) into a recognizable format. Processing may take place internal to the collection device. Depending on the signal, multiple processing activities may be required, some internal to the device and others external to the device. Some or all the processing may occur via “reachback” to other locations.

Signals Intelligence exploitation methods are applied to processed SOIs. This results in either a man readable or computer readable collection report, which is provided to SIGINT analysts. Man readable collection reports include transcriptions and translations, while computer readable reports include data files. Exploitation may occur at the same locations as collection and/or processing, or from a location physically separated from either step. The output to SIGINT analysts remains raw SIGINT and must be protected in accordance with United States signals intelligence directives (USSIDs).

Marine Corps tactical SIGINT units provide trained personnel and equipment for SIGINT collection teams, with the intent to integrate collection, processing, and exploitation as close to the point of intercept as possible. This measure reduces the time it takes to understand a collected signal’s relevance and value. MAGTF SIGINT collection teams generally operate in close coordination with battlespace owners and usually operate in general support (GS) of the MAGTF, tasked as part of the overall MAGTF collection plan. As such, the teams may receive specified tasking that includes providing indications and warnings to adjacent or supported units.

These units often exercise tactical control over the teams. Detailed planning and resource management is required to ensure MAGTF SIGINT operations are optimized and the commander's requirements are met.

The evolution of the SIGINT operating environment makes it increasingly difficult to integrate collection, processing, and exploitation capabilities into a single collection team. Size, weight, power requirements, and cooling are the major factors considered when developing and deploying a SIGINT collection system. When the capabilities cannot be integrated into one site, a separate location will be utilized for processing and exploitation. High-capacity, low-latency Sensitive Compartmented Information (SCI) networks are required for communications between separated sites. Despite network availability, communications between separated sites may experience timeliness and latency issues, thus delaying the exploited signal's delivery and potentially degrading its usefulness and intelligence value.

Cryptologic language analysts (Military Occupational Specialty [MOS] 264X/27XX) are vital during signal processing and exploitation. Cryptologic language analysts are trained in languages most relevant to MAGTF operations and are a high-demand, low-density resource.

Signals Intelligence Collection. Signals collection is a broad function and not necessarily confined to SIGINT operations. SIGINT authorities, granted by the Director of the National Security Agency (DIRNSA), govern the SIGINT process. When a signal is collected for SIGINT purposes by SIGINT personnel or through SIGINT processes, it falls under SIGINT authorities. The Marine Corps divides SIGINT collection into the following three sub functions:

- Survey (search).
- Collection (acquire).
- Signal geolocation (location).

Surveys are categorized by the nature of the search performed. Spectrum surveys are EMS searches to identify active frequencies. Signal surveys identify the type of communications technology that is active on a frequency or range of frequencies. Network surveys are used to identify wired or wireless networks' technical details.

From both a COMINT and ELINT perspective, collection consists of intercepting, acquiring, and storing raw electronic signals that require processing to become useful intelligence. Signals analysis may be necessary to determine signal type and decoding requirements.

Signal geolocation is used to determine the position of a transmitter and is based on a signal's externals (parametric information) rather than its internals (content). The transmitter may be a node in an adversary's military or government, a non-hostile system of a friendly group, or the system of an individual in a loosely organized asymmetric or transnational criminal network. Before an operator or analyst determines a geolocation's intelligence value to the MAGTF, the signal content must be analyzed, or the relationship of the signal to other known signals must be understood.

Signals Intelligence Processing. The process of encoding information signals into a carrier wave for transmission at higher frequencies is called modulation. The process of decoding this information on the receiving end of the transmission is demodulation. For pulsed signals, the pulses are modulated signals on a carrier wave. Continuous-wave signals may be either modulated or unmodulated. During the processing phase, raw electronic signals (communication and non communication) are deconstructed (i.e., deinterleaved, demodulated, and/or decrypted) into recognizable signals and formats.

Communication signals (e.g., radios, cell phones, and computers) are demodulated and decrypted into voice or text signals. When processing is complete for a communication signal, the signal format can be identified (e.g., cellular, trunk/digital mobile radio, wi-fi, push to talk, etc.) Non communication signals (e.g., radar, data links, microwaves) may consist of either pulsed or continuous wave signals. Exploitation often requires a cryptologic language analyst to listen and transcribe live or recorded voice or translate text. This is commonly called gisting.

Pulsed signals, commonly referred to as ELINT signals, consist of rapidly changing amplitude values. When many pulsed signals are collected per second on the same frequency, they become interleaved (i.e., mixed), and individual signals may be difficult to isolate. Before individual signals can be reconstructed, the pulses must be deinterleaved (i.e., separated).

Continuous-wave signals are periodic waveforms with constant amplitude and frequency. The waveform characteristics make continuous wave signals easier to characterize than pulsed signals.

Exploitation. Electronic intelligence exploitation is the parametric characterization of the external attributes of a processed ELINT signal. These parameters include the following:

- Frequency.
- Pulse Duration.
- Pulse Repetition Frequency.
- Pulse Repetition Interval.
- Pulse Width.
- Scan Type.
- Scan Rate.

Geolocation Methods

The Marine Corps categorizes signal geolocation in three ways:

- Direction finding (DF).
- Passive geolocation.
- Precision geolocation (PGL).

Direction finding, passive geolocation, and PGL operations are most effective when conducted as part of the SIGINT process. Geolocation operations require detailed planning to ensure SIGINT operations are optimized to support geolocation activities and during intelligence operations are executed in response to PIRs.

If non SIGINT units conduct signal geolocation activities, then a close relationship with a SIGINT analytic node and an appropriately secure reporting link must be established to determine whether the targeted signals are signals the MAGTF deems important. Users, frequencies, and modes of communication constantly change, making the characterization of a signal difficult without understanding the internals and the user's relationship to MAGTF operations (i.e., friend or foe). SIGINT units have access to many resources that assist with characterizing and geolocating.

Direction Finding. Marines conduct DF operations to determine a radio wave’s direction of arrival (DOA). DF is a valuable tool for military commanders, used for finding and fixing transmitters used by people and systems of interest. Specifically, DF can be used to determine people and equipment movements, weapons systems locations, or targets for jamming or intercept.

Direction Finding is not a precise science, primarily due to radio wave propagation and the numerous factors impacting a radio wave after leaving the transmitting antenna. Accurately locating a signal using DF requires specialized equipment and detailed planning, including battlespace placement of DF assets. Equipment sensitivity, weather, terrain, and enemy actions are all factors that impact DF accuracy. Collection teams are trained in on site exploitation and establishing a DF baseline, enabling them to locate a transmitter within an operationally relevant timeline.

Direction Finding operations are executed to provide force protection, indications and warnings (I&W) or support an intelligence operation. The team providing DF support is typically integrated with the unit receiving I&W and force protection support. Supporting units provide logistics support and security for the DF team.

Many factors affect the signal and the ability to conduct accurate DF operations. DF is most accurate from a fixed site using a high-gain directional antenna that can determine the point of origin for a radiated power source. As shown in figure 2-1, a Yagi antenna has pronounced directionality, so a transmission source can be determined simply by pointing the antenna in the direction of the greatest signal strength.

Figure 2-1. Yagi Antenna

Multiple antenna elements configured as an array (shown in figure 2-2) are also used to identify a signal's DOA by determining the angle of arrival, shown in figure 2-3.

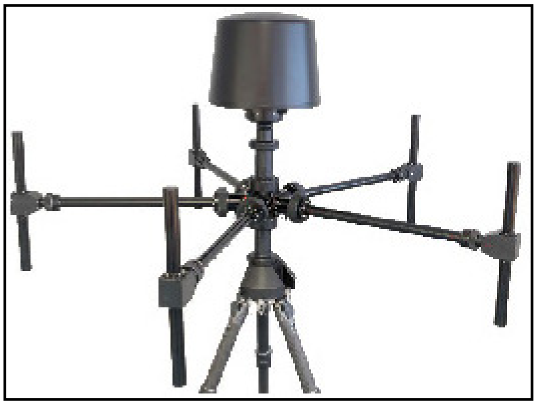


Figure 2-2. Direction Finding Array

Direction finding provides one or more lines of bearing (LOBs) used to determine an SOI's DOA. A LOB is a straight line (or azimuth) from the DF equipment to the transmitting antenna. Evaluating the received voltage can determine the SOI's direction.

A single LOB will only approximate the direction of a transmitter. However, this may be enough to provide a cardinal direction to the adversary or help determine if the adversary is on the move. It can also be correlated to existing information, such as order of battle information or existing LOBs, to refine a transmitter's location.

Different DF sites must take multiple LOBs to refine a transmitter's location. Then, by plotting the LOBs, or azimuths, from each site toward the transmission's DOA, the point where those lines cross is the transmitter's approximate location (see figure 2-3).

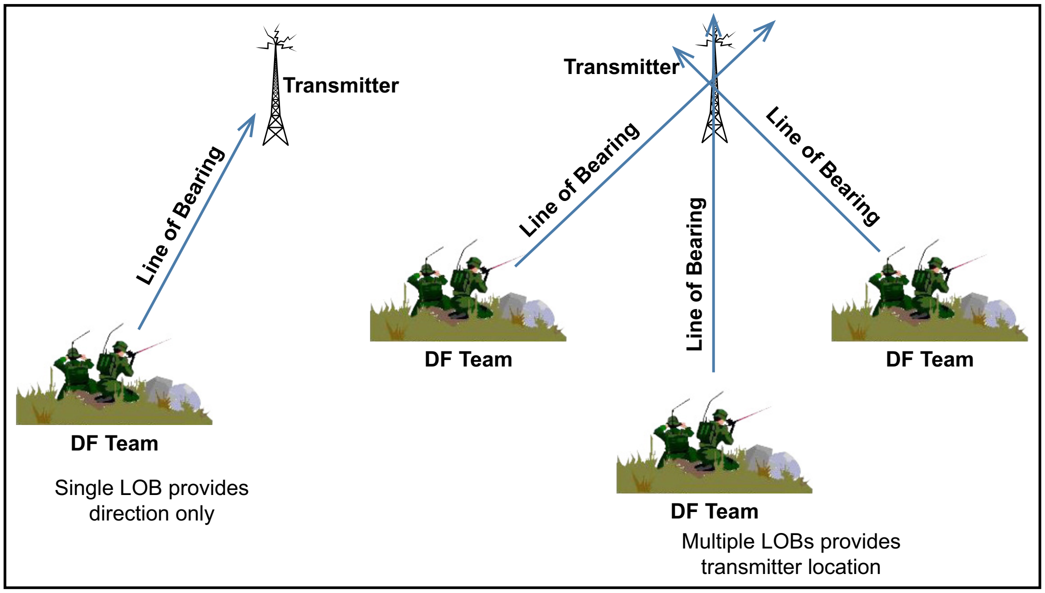


Figure 2-3. Lines of Bearing

Passive Geolocation. In the Marine Corps, determining geolocation through passive means is preferred. Passive geolocation protects friendly force locations and the integrity of friendly capabilities—it should always be the first and primary method used to locate a target. Passive geolocation methods include time difference of arrival (TDOA) and frequency difference of arrival (FDOA). TDOA compares the difference in time when a signal emission reaches different receiving elements, whereas FDOA compares the frequency shift as captured by receivers in motion.

Both TDOA and FDOA geolocation operations provide more precise locations when LOBs are based on an SOI's received voltage. TDOA and FDOA methods are often more accurate due to multilateration, which is a situation where multiple receivers, working together, reduce environmental effects such as multipath interference.

The TDOA is a measurement of the difference in time between two stations receiving the same signal (see figure 2-4). Precise station locations and time measurements are necessary to provide accurate TDOA results. The TDOA measurement is used to calculate a geographic estimate of the emitter. With a third station, a second TDOA measurement will produce a second geographic shape. The geographic points that the two calculations share will result in an estimated location (i.e., an elliptical or circular area of probability).

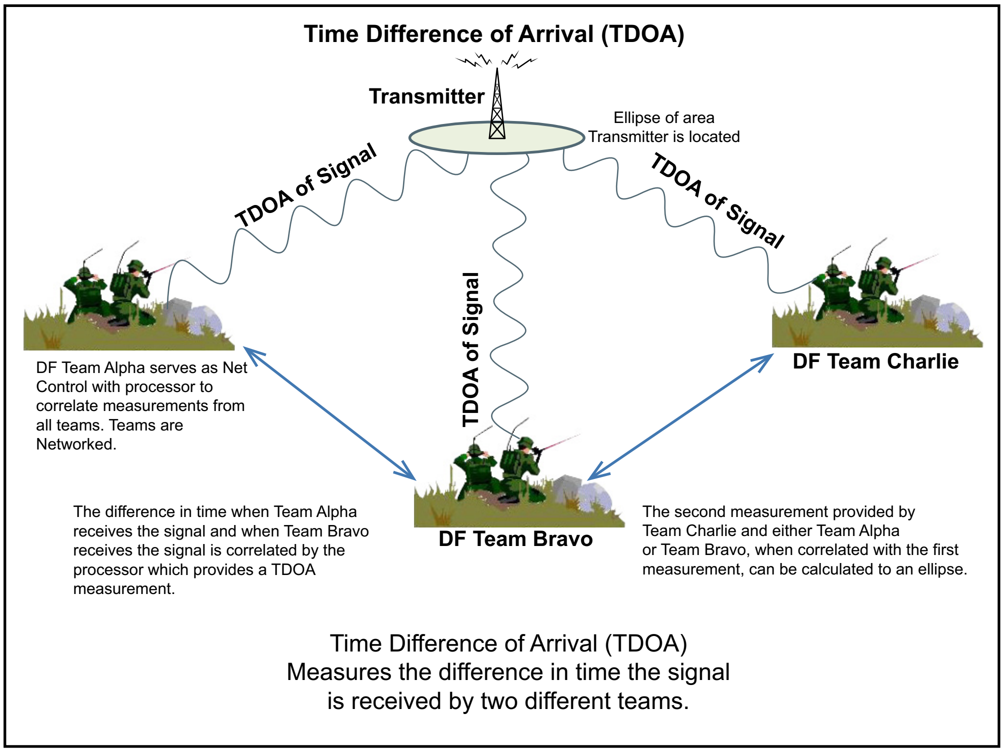

Time Difference of Arrival (TDOA)
Transmitter
Ellipse of area Transmitter is located
TDOA of Signal
TDOA of Signal
TDOA of Signal
DF Team Alpha serves as Net Control with processor to correlate measurements from all teams. Teams are Networked.
DF Team Charlie
DF Team Bravo
The difference in time when Team Alpha receives the signal and when Team Bravo receives the signal is correlated by the processor which provides a TDOA measurement.
The second measurement provided by Team Charlie and either Team Alpha or Team Bravo, when correlated with the first measurement, can be calculated to an ellipse.
Time Difference of Arrival (TDOA) Measures the difference in time the signal is received by two different teams.

Figure 2-4. Time Difference of Arrival

The FDOA is the measured difference in frequencies collected by multiple stations due to the Doppler effect (shift in received frequency due to the transmitter or receiver's movement). This shift occurs due to an increase (or decrease) in a signal's frequency as either the source and/or receiver move in relation to each other. The collection team's and the emitter's relative motion is essential to obtain an accurate FDOA location. Stationary receivers can contribute to an FDOA result; however, at least one receiver must be moving at a high rate.

Precision can be increased by combining TDOA and FDOA methods as they are complementary. TDOA provides accuracy in bearing, while FDOA provides accuracy in range estimation. This method provides a quicker location calculation versus calculating location by one method alone (i.e., DOA, FDOA, or TDOA). This method also requires fewer measurements, which increases the probability of locating an SOI even when the user is practicing operational security and limiting transmission times. Three to five FDOA or TDOA sensors provide the best location results, as too many sensors will dilute results by introducing ambiguity.

A combination of TDOA and FDOA can provide a geolocation estimate with only two sensors, but it requires a minimum of one airborne sensor. A quick and accurate location can be calculated when a TDOA/FDOA location is combined with an algorithm that accounts for elevation, geography, and amplitude. An analyst should review all automatically generated location estimates for accuracy before distributing the information.

Precision Geolocation. The PGL methods are classified details that are available on appropriately cleared networks.

Geolocation Method Employment. The Marine Corps organizes, trains, and equips MAGTF SIGINT collection teams to execute DF and passive geolocation operations. An effective geolocation effort requires close coordination between collection and geolocation sites and network control. This arrangement is optimal so that in dynamic, complex SIGINT operational environments, signals can be characterized and verified as valid targets before teams execute DF or passive geolocation operations. Under ideal conditions, DF and passive geolocation assets array in a predetermined baseline consisting of at least three collection and geolocation stations networked together. One node may act as the geolocation network control, although the network control does not necessarily have to be one of the geolocation stations. The addition of an airborne asset to the geolocation network will provide a greater variety of measurements. Regardless of the network composition, node placement is critical to ensure all stations can "hear" the transmitter and the network control node.

Prompted by the intelligence community, the DOD established the Theater Net centric Geolocation (TNG) network. The TNG increases the number of LOBs or measurements and reduces the margin of error in geolocation operations through common precision timing and location standards, automated tipping and cueing mechanisms, and a common geolocation reporting network for national, theater, and tactical location assets. These cooperative geolocation capabilities allow the MAGTF to obtain timely and accurate locations without saturating an area of operations (AO) with geolocation assets. A MAGTF's ISR assets must integrate with the TNG to benefit from it.

Signals Intelligence Analysis and Production

A US Government element must be a SIGINT production chain (SPC) member to analyze and produce SIGINT information. Members of an SPC are assigned a valid SIGINT mission by the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), or the

SIGINT Director. Members of an SPC must document enabling, production, or oversight activities in a unit's USSID, a site profile referenced in another USSID for field elements, or in a mission and activities statement for headquarters elements. Collecting, processing, or exploiting certain signals is not strictly a SIGINT function. However, analyzing collection reports and characterizing signals is governed by laws and policies and is a distinct function of SIGINT.

Signals Intelligence analysts use SIGINT information from organic (i.e., MAGTF owned) and non-organic (e.g., Joint, National, etc.) collection sources to develop a SIGINT view of an area of responsibility or AOR. This view may stem from a single report, a single source, or many reports from many sources. SIGINT analysts may leverage national SIGINT data to reference and research the analytical task supporting PIRs/IRs. SIGINT analysts use multi discipline intelligence to assist their analytic efforts or create a more detailed product. SIGINT analysts cannot provide fused intelligence products; fused products are the responsibility of all source analysts.

Those within the MAGTF who consume tactical Marine SIGINT can expect sanitized reporting that supports force protection, I&W, or PIRs. MAGTF intelligence personnel receive more detailed reporting to support all source analysis.

Signals Intelligence Dissemination, Integration, Evaluation, and Feedback

The senior SIGINT component within the operating forces, typically a radio battalion (RadBn) Operations Control and Analysis Center (OCAC) or US Marine Special Operations Command (MARSOC) Direct Support Team (DST), is responsible for disseminating all SIGINT ISO MAGTF intelligence requirements. The OCAC/DST must adhere to all guidelines regarding access to raw SIGINT and sanitized reporting. The RadBn and MARSOC Intelligence Battalion maintain distribution lists for units approved to receive SIGINT information. SIGINT analysts collaborate with all source analysts to ensure SIGINT is included in all source intelligence picture, while the OCAC/DST ensures overall proper SIGINT use. Integrating SIGINT throughout the intelligence process is a best practice yielding better SIGINT products and support.

All SIGINT and intelligence elements are responsible for evaluating SIGINT use and providing feedback. It is important that SIGINT and intelligence elements follow up with supported units to ensure those units' information needs are met within adequate timelines.

Signals Intelligence in Support of Cyberspace Operations and Electromagnetic Warfare

Cyberspace Operations

Cyberspace is a global domain within the information environment, consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

Cyberspace operations are the employment of cyber capabilities, where the primary purpose is to achieve objectives in or through cyberspace. Such operations include offensive cyberspace operations, defensive cyberspace operations, and activities to operate and defend the Department of Defense information network (DODIN).

Computer network exploitation (CNE) enables operations and intelligence collection capabilities conducted using computer networks to gather data from target or adversary automated information systems or networks.

In RadBns and the MARSOC Intelligence Battalion, the tactical employment of CNE and computer network attack-related capabilities is limited and requires special permissions from DIRNSA. These special permissions are requested through the Marine Cryptologic Office located at NSA/CSS. For additional information about the Marine Cryptologic Office, see chapter 4, SIGINT community.

All cyber network operations require close relationships with national entities and US Marine Forces Cyberspace Command (MARFORCYBERCOM). These close relationships come with extra processes and regulations, but they allow the Marine Corps to leverage significant capabilities.

Electromagnetic Warfare

Electromagnetic Warfare (EW) is action involving the use of electromagnetic and directed energy to safeguard friendly use of the EMS while denying or degrading adversary use of the same. EW consists of three divisions:

- Electromagnetic attack (EA).
- Electromagnetic protection (EP).
- Electromagnetic warfare support (ES).

Electromagnetic attack is the division of EW that focuses on denial, degradation, deception, and disruption of adversary electromagnetic spectrum employment. EA is considered a form of fires and must be coordinated as such before its employment.

Electromagnetic protection focuses on protecting friendly electromagnetic spectrum use. Although EP responsibility is external to SIGINT efforts, it absolutely informs SIGINT efforts for collection, ES, and EA.

Electromagnetic warfare support is the division of EW involving actions tasked by, or under the direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for immediate threat recognition, targeting, planning, and conducting future operations, and other tactical actions such as threat avoidance and homing.

Electromagnetic warfare support is strictly limited to analysis to support I&W and time-sensitive targeting. The distinction between SIGINT and ES depends on the entity tasking or controlling the collection assets, the tasking, and the purpose. However, the same assets and resources tasked with ES can simultaneously collect SIGINT that meets other collection requirements.

Put another way, the difference between SIGINT and ES is the purpose of collection and analysis. When data is collected to provide security or guide a force to a target, it is ES. On the other hand, data that is vetted, analyzed, retained for over 24 hours, or collected to inform operations, such as adversary activity, is considered intelligence.

SIGNALS INTELLIGENCE EMPLOYMENT

The DIRNSA is the US Government Community Functional Manager for all SIGINT (as per US Code Title 50, Executive Order [EO] 13470, and National Security Council Intelligence Directives [NSCID]). These documents provide DIRNSA the authority to regulate the technical development and employment of all SIGINT assets within the US Government. The DIRNSA delegates SIGINT operational tasking authority (SOTA) to Marine Forces (MARFOR) commanders to conduct SIGINT operations within their AOs. However, the DIRNSA specifically retains the right to exercise control over digital network intelligence (i.e., CNE). As a result, tactical SIGINT elements must request permission each time they desire to perform a collection mission against computer networks. The MARFOR commander may delegate SOTA to the MAGTF commander, who maintains operational control (OPCON) of Marine SIGINT assets. SIGINT collection is directed by the RadBn commanding officer (CO) or a detachment officer-in-charge (OIC).

The MAGTF commander must also receive mission delegation to conduct SIGINT operations. Mission delegation is another authority granted by the DIRNSA to tactical SIGINT units to access many of the tools, equipment, and NSA/CSS databases necessary to accomplish their SIGINT mission. Requests for mission delegation are submitted to the Marine Cryptologic Office, who then submits the request to the appropriate NSA/CSS office of responsibility and advocate for approval.

Signals Intelligence may be planned and executed as part of the greater intelligence plan or as a separate discipline, and it may be in GS or direct support (DS) to a unit. Because of SIGINT relationships and robust national capabilities, when supporting a MAGTF or MAGTF element, SIGINT units may be required to inhabit an area not associated with the physical space the supported unit occupies. Also, SIGINT units require bandwidth over communications paths to provide support.

In a GS relationship, the MAGTF establishes SIGINT priorities in support of the force as a whole. Given the nature of SIGINT operations, GS is the most common support relationship that allows for SIGINT support to the host unit and MAGTF SIGINT requirements. A SIGINT element may accompany a supported unit on a mission and require host unit support but still be attached and in GS to the MAGTF.

In a DS relationship, the SIGINT unit is required to support another specific force and is authorized to answer directly to the supported force’s requests for assistance. When required by the mission and situation, the SIGINT unit, or an element, may place some teams in DS and others in GS.

CHAPTER 3. SIGNALS INTELLIGENCE AUTHORITIES, OVERSIGHT, TASKING, AND CONTROL

The Marine Corps SIGINT community consists of members from within the operating forces, Training and Education Command (TECOM), Marine Corps Systems Command (MARCORSYSCOM), Combat Development and Integration (CD&I), and at Headquarters Marine Corps (HQMC). It exists to support the MAGTF as a core component of the Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise (MCISRE).

The Marine Corps SIGINT community is also an integral component of the USSS. The USSS consists of all national, theater, and tactical SIGINT capabilities working in concert to provide a more complete SIGINT picture to “customers,” ranging from the infantry squad leader to the President of the United States.

Being part of the USSS allows the Marine Corps SIGINT community to leverage the vast resources of the intelligence community (IC) to provide the MAGTF with intelligence, combat information, and targeting data that would otherwise be unavailable. In return, the Marine Corps is required to commit manpower to the national agency; follow National Security Agency (NSA) policies regarding the acquisition, handling, and dissemination of SIGINT data and products; and feed SIGINT to the USSS, even when conducting SIGINT operations solely in support of the MAGTF.

PEDIGREE OF SIGNALS INTELLIGENCE AUTHORITIES

The SIGINT authorities flow from the US Constitution through various statutes (Title 10, Title 40, Title 50 United States Code), Presidential and National Security Council Directives, and Department of Defense Instructions (DODIs) and Directives to the DIRNSA/CHCSS. He is responsible for unifying US Government SIGINT activities into one organization. While one organization does not exist, the USSS is effectively a unified enterprise where the DIRNSA/CHCSS controls the activities of SIGINT organizations down to the smallest tactical teams. The DIRNSA/CHCSS exercises SIGINT OPCON over the USSS via USSIDs. SIGINT OPCON and the USSID systems are how the DIRNSA/CHCSS manages and controls the enterprise and delegates authorities to MAGTF SIGINT units.

LAWS

The two sections of the United States Code that affect Marine Corps SIGINT are Title 10 and Title 50.

United States Code Title 10

Title 10 is the ‘Armed Forces’ section of US law and provides the legal basis for the Services' roles, mission, and organization. It is frequently referred to as “the authority to organize, train, and equip.”

Title 10 provides the Commandant of the Marine Corps (CMC) the authority to create and train SIGINT Marines and units, develop and procure SIGINT systems, and develop TTPs for SIGINT Marines to accomplish tactical military operations. As stated previously, the Marine Corps SIGINT mission is beholden to DIRNSA/CHCSS. The CMC retains significant authority under Title 50 over how SIGINT Marines are trained in formal schools, what equipment SIGINT Marines can use to conduct SIGINT operations, and when, where, and how the Marine Corps conducts SIGINT operations.

Title 10 also sets the guidance and responsibilities for intelligence oversight and handling, which is covered in greater detail later in this chapter.

United States Code Title 50

Title 50 of the United States Code outlines the Services’ role in war and defense. Title 50 also contains most laws relating to intelligence.

Title 50 describes intelligence and its sub categories and defines intelligence-related terms. It identifies the members of the intelligence community, their sub-elements, and the roles and responsibilities of each. Title 50 details the roles of the Secretary of Defense (SecDef), Under Secretary of Defense for Intelligence (USD[I]), Director of National Intelligence (DNI), and DIRNSA.

Title 50 appoints SecDef as the executive agent of SIGINT for the US Government (the SecDef delegates this authority to the DIRNSA). Title 50 also appoints the DIRNSA as the US Government lead for cryptology, which, along with SIGINT, includes information assurance (IA) responsibilities.

Policies and Directives

While the United States Code serves as the foundation of intelligence authorities, the implementation of laws found in Title 10 and Title 50 lie in Executive Branch policies and directives. The following documents define the legal roles, authorities, and responsibilities of the DIRNSA/CHCSS over the USSS that include USMC SIGINT activities.

The Truman Memorandum. The Truman Memorandum of 24 October 1952 established the NSA as the centralized authority for US COMINT activities. Implemented through a series of NSCIDs, Department of Defense (DOD) memoranda, and Department of Defense directives (DODDs), the Truman Memorandum appointed SecDef as the Executive Agent for COMINT for the US Government.

Executive Orders and National Security Council Intelligence Directive 6. Executive orders are directives issued by the president for managing federal government operations. There are several EOs that pertain to tactical Marine Corps SIGINT capabilities, such as—

- EO 12333 details intelligence community activities.
- EOs 13355 and 13470 add amendments to EO 12333.

These EOs detail the intelligence and intelligence related responsibilities, authorities, duties, and accountability to decision makers. They also list the departments' and agencies' responsibilities to prepare and provide intelligence in a manner that allows the full and free exchange of information.

Additionally, these EOs detail foreign intelligence collection and appoint the DIRNSA as both the functional manager and US Government lead for SIGINT. They also specify the responsibilities and authorities of the NSA, which include the following:

- Collecting (including through clandestine means), processing, analyzing, producing, and disseminating SIGINT information and data for foreign intelligence and CI purposes in support of national and departmental missions.
- Establishing and operating an effective, unified organization for SIGINT activities, except for the delegation of OPCON over certain operations that are conducted through other elements of the intelligence community. No other department or agency may engage in SIGINT activities unless authorized by SecDef, after coordination with the director.
- Controlling SIGINT collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders.
- Providing SIGINT support for national and departmental requirements and conducting military operations.
- Prescribing security regulations covering operating practices, including the transmission, handling, and distribution of SIGINT and communications security material within, and among, the elements under control of DIRNSA, and exercise the necessary supervisory control to ensure compliance with the regulations.

National Security Council Intelligence Directive 6, *Signals Intelligence*, originally issued 15 September 1958 and later revised on 17 February 1972, details the SIGINT mission and authority of the NSA under the SecDef and established more direction for the conduct of United States SIGINT activities. Specifically, it—

- Defines the SIGINT mission and authority of NSA under SecDef.
- Assigns responsibility for the SIGINT mission to DIRNSA.
- Creates a CSS, under DIRNSA, which included SIGINT functions previously performed by various military departments and other United States governmental elements engaged in SIGINT activities.

The 1972 revision also provides that the DIRNSA "shall exercise full control over all SIGINT processing and collection activities," except as follows:

> *Operations of mobile SIGINT platforms are to be exercised through the military command structure. However, the DIRNSA is authorized to issue mandatory instructions and assignments directly to such platforms, subject only to appeal by SecDef.*

Further DOD implementation of the EOs and NSCID 6 established the DIRNSA/CHCSS's authorities over tactical SIGINT platforms. The SecDef limits the DIRNSA's authorities to allow military commanders a reasonable expectation that organic SIGINT capabilities are authorized to support local tactical commanders' objectives. However, the organic SIGINT units must follow NSA policies and procedures to safeguard US persons' rights and protect SIGINT sources and methods.

Department of Defense Directive 5100.20. DOD Directive 5100.20, National Security Agency (NSA)/Central Security Service (CSS), revised and signed 26 January 2010, states no other organization within the DOD shall engage in SIGINT activities, except when directed or delegated by the SecDef or the DIRNSA/CHCSS after coordination with the DNI. The DODD provides specified tasks to the DIRNSA/CHCSS as well as the secretaries of the military departments.

In the document, the DIRNSA/CHCSS is specifically delegated authority by the SecDef to—

- Serve as the principal advisor to the SecDef, the Chairman of the Joint Chiefs of Staff, and the combatant commanders on SIGINT, under the authority, direction, and control of the USD(I).
- Establish and operate an effective, unified organization for SIGINT activities, including executing any SIGINT-related functions as directed by the SecDef.
- Exercise SIGINT OPCON and establish policies and procedures for departments and agencies to follow when appropriately performing SIGINT activities for the SIGINT mission of the United States to be accomplished in the most efficient and effective manner. In the case of service mobile SIGINT platforms, systems, or assets used to collect SIGINT, the DIRNSA/CHCSS shall direct movement requirements through appropriate channels to the military commanders, who shall retain responsibility for operational command of the platforms.
- Provide technical guidance and assistance to all USG SIGINT or SIGINT related operations.
- Provide guidance, as directed by the USD(I), to the secretaries of the military departments and the Commandant of the United States Coast Guard to effect and ensure sound and adequate military and civilian cryptologic career development and training programs; develop cryptologic knowledge and skill standards; and conduct or otherwise provide for necessary specialized and advanced cryptologic training, pursuant to DODI 3305.09.
- Provide linguistic and other training for cryptologic personnel as outlined in Public Law 86 36.
- Serve as the executive secretary for deconfliction processes for offensive cyber operations and exploitation activities as specified by memorandum of agreement among the DOD, the Department of Justice, and other members of the IC.

Department of Defense Directive 5200.10. DODD 5200.10 tasks the Secretaries of the Military Departments with the following:

- Assigning military personnel, including US Coast Guard, to NSA/CSS, pursuant to approved Joint Manpower Program authorizations as prescribed by the Office of the Secretary of Defense (OSD), the Chairman of the Joint Chiefs of Staff, and the Commandant of the US Coast Guard.
- Designating an organization within each respective military service, including the US Coast Guard, as a service cryptologic component (SCC). The designated organization shall serve as the primary Service authority for all operations, programming, budgeting, training, personnel, policy, doctrine, and foreign relationships for cryptologic activities. The SCC will also have administrative and logistical responsibility for the military Service or US Coast Guard cryptologic workforce assigned to missions funded by NSA/CSS.
- Assigning, after consulting with the DIRNSA/CHCSS, the commander/chief of their SCC who is usually of at least one-star rank (or equivalent civilian grade). The commander/chief of the SCC shall be subordinate to the CHCSS for all cryptologic matters.
- Providing personnel trained to cryptologic training system standards, and fully cleared in accordance with DIRNSA/CHCSS standards, for assignment across the NSA/CSS enterprise to include standing task forces.

DOD Directive 5200.10 provides significant authorities to the commander or chief of the SCC. The commander or chief of each SCC is the primary authority for all operations, programming, budgeting, training, personnel, policy, doctrine, and foreign relationships for cryptologic activities. Subordinate to the CHCSS for cryptologic matters, the role and authority of the commander or chief of the SCC is to ensure the Service SIGINT assets are operating in accordance with DIRNSA/CHCSS SIGINT technical and operational policies, directives, and guidance. To that end, the commander or chief of the SCC has the authority to levy requirements on the combat development process to specify capabilities that may or may not be used in accordance with NSA/CSS policies. In rare cases, the commander or chief of the SCC has the authority to direct certain capabilities or technologies that must be inserted into programs of record to meet NSA/CSS standards or direct the use of NSA/CSS systems instead of commercial-off-the-shelf systems.

In 2009, the Undersecretary of the Navy and the Assistant Commandant of the Marine Corps formally designated the Director of Intelligence (DIRINT) as Chief of the Marine Corps Cryptologic Component. The DIRINT is responsible and accountable to the CMC and DIRNSA/CHCSS for Marine Corps SIGINT functions specified in DODD 5200.10 as well as DODI O 3115.07, *Signals Intelligence*.

Department of Defense Instruction O-3115.07. DOD Instruction O-3115.07, *Signals Intelligence*, updates SIGINT policy, definitions, and responsibilities within the DOD. It established as DOD policy SIGNT instructions on collection, processing, analysis, production, and dissemination activities issued by the DIRNSA/CHCSS shall be mandatory for all DOD Components and other non-DOD entities that are conducting SIGINT under SecDef authority. These provisions are subject to an appeal to SecDef where appeal adjudication is delegated to the USD(I).

The instruction further directs the DIRNSA/CHCSS to—

- Exercise SIGINT OPCON over SIGINT activities of the USSS in accordance with DODD 5200.10 to respond most effectively to military and other SIGINT requirements by:
  - Delegating standing SOTA to the military departments, the CMC, and the Commandant of the USCG with organic SIGINT units permanently assigned under their command.
  - Delegating temporary SOTA through the Chairman of the Joint Chiefs of Staff to the combatant commanders, subordinate component commanders, joint task forces, and directly to the SCC on a case by case, mission specific basis to permit those commanders (or delegated representatives) to directly task designated SIGINT units, platforms, and assets assigned to their command to achieve their mission objectives in a timely and efficient manner, and coordinating these actions with the SCCs so as not to impinge upon the capabilities of organic tactical SIGINT units to provide required support to their parent Service.
  - Approving SIGINT missions for military SIGINT units, platforms, or other assets assigned to and under OPCON of a military commander.
  - Levying SIGINT advisory tasking against military units, platforms, or other assets that have SIGINT capabilities but whose primary purpose is not SIGINT collection, processing, or other SIGINT-related activities. This tasking must:
    - Have the concurrence of the affected commander.
    - Not interfere with the primary purpose of the resource or the mission of the command to which it is assigned.
    - Provide guidance to ensure the resulting SIGINT product is provided to the designated NSA/CSS office or activity as soon as possible.
  - Levying SIGINT supplemental tasking against military SIGINT units, platforms, or other assets for which SOTA has been delegated to a military commander with the concurrence of the affected commander.
  - Retaining SIGINT OPCON of all SIGINT resources fulfilling national SIGINT requirements.
  - Appraising the combatant command Joint Intelligence Operations Centers and Defense Intelligence Operations Coordination Center of all SIGINT-related activities relevant to their respective responsibilities.
  - Upon approval by the USD(I), develop and implement SIGINT programs, plans, policies, procedures, principles, and guidance for DOD elements engaged in SIGINT activities in accordance with DOD policies and guidance to:
    - Provide technical guidance for the collection, processing, analysis, production, and dissemination of SIGINT.
    - Issue SIGINT operational and technical policy to carry out DIRNSA/CHCSS responsibilities and functions to units involved in SIGINT operations, keeping the USD(I) and the DNI informed. This includes issuing instructions and policies related to collecting, processing, analyzing, producing, retaining, disseminating, and assessing SIGINT information.
    - Exercise the necessary monitoring and supervisory control to ensure compliance with DOD and DNI issuances prescribing security regulations and with directives covering SIGINT operating practices, including transmitting, handling, and distributing SIGINT material.
  - Standardize SIGINT equipment, processes, and facilities; eliminate unwarranted duplication of SIGINT efforts, where practical, in coordination with the military departments.

DODI O-3115.07 directs the Marine Corps through the Secretary of the Navy to accomplish specific tasks. The designated officer or organizations responsible to the CMC for executing the tasks are identified in parentheses. The tasks are as follows:

- Plan and program for defense SIGINT capabilities under the guidance of the USD(I) and in coordination with DIRNSA/CHCSS (DIRINT).
- Designate an SCC commander for each Military Service and provide military personnel to NSA/CSS to perform NSA/CSS-assigned SIGINT missions in accordance with approved requirements and procedures (DIRINT, Marine Cryptologic Support Battalion [MCSB]).
- Operate and maintain SIGINT facilities and resources, in coordination with NSA/CSS, for the conduct and support of SIGINT operations as authorized and directed by SecDef or the USD(I), including military reserve programs to meet emergency or wartime requirements for SIGINT resources (DIRINT, MARFORs).
- Coordinate SIGINT investment programs with DIRNSA/CHCSS. In the event of an issue or disagreement with DIRNSA/CHCSS, submit an appeal to the USD(I) for resolution (DIRINT, SYSCOM).
- Develop network-enabled SIGINT equipment that meets architecture standards and is interoperable with national SIGINT systems, other Military Department tactical SIGINT systems, and Joint Intelligence Operations Center operating systems, as necessary (DIRINT, CD&I, SYSCOM).
- As appropriate and in accordance with guidance from DIRNSA/CHCSS, through the respective military department SIGINT and training organizations, conduct SIGINT activities, training, and operations in support of military commanders and DIRNSA/CHCSS (DIRINT, TECOM, MARFORs, MCSB).
- Assist NSA/CSS in conducting SIGINT related research and development to meet the needs of the United States for SIGINT by—
  - Coordinating research development test, and evaluation (RDT&E) requirements with DIRNSA/CHCSS (DIRINT).
  - Accomplishing specified RDT&E tasks within approved programs as requested by DIRNSA/CHCSS and in accordance with DOD guidance and direction (DIRINT).
  - Maintaining a system in coordination with DIRNSA/CHCSS to support SIGINT management by reporting program execution data to NSA/CSS (DIRINT).
  - Performing threat analysis and coordinating with other DOD components, as necessary, to incorporate SIGINT threat countermeasures in acquisition and RDT&E programs (DIRINT, Marine Corps Intelligence Activity [MCIA], MARCORSYSCOM).
  - Coordinating, planning, programming, budgeting, maintaining, and conducting SIGINT training in accordance with DODI 3305.09 DOD Cryptologic Training and USD(I) policy and guidance (DIRINT, TECOM).
  - Submitting SIGINT information requirements to Defense Intelligence Agency (DIA), simultaneously providing information copies to NSA/CSS. In addition, submit time-sensitive or otherwise urgent SIGINT information needs directly to NSA/CSS, simultaneously informing the Defense Intelligence Operations Coordination Center (DIRINT, MCIA).

SIGNALS INTELLIGENCE OVERSIGHT REQUIREMENTS

Intelligence oversight is the process of ensuring that DOD intelligence, CI, and intelligence-related activities are conducted in accordance with all applicable US laws, Presidential Executive Orders, and DOD directives and regulations. It also ensures that intelligence personnel do not collect, retain, or disseminate information about US persons unless done in accordance with specific guidelines, proper authorization, and within only specific categories. Intelligence oversight has the following two main objectives:

- The prevention of violations, whether intentional or unintentional.
- The process for dealing with violations when they occur.

Intelligence oversight has purview over intelligence personnel, intelligence operations, and any information collected during intelligence-related activities. In some cases, information collected by non-intelligence personnel for non-intelligence reasons may also fall within the purview of intelligence oversight. For more information, refer to the following:

- EO 12333.
- DOD Dir 5240.01.
- DOD Reg 5240.1-R.
- SECNAVINST 3820.3E.
- MCO 3800.2B.

As described in Chapter 2, combat information is not necessarily intelligence and may be collected by non intelligence personnel. When the information is collected by non intelligence personnel for non intelligence reasons, it may provide situational awareness or knowledge to a commander and may be used without falling under the purview of intelligence oversight. If stored or evaluated, however, it becomes intelligence and is subject to intelligence oversight. This is of specific interest to the SIGINT community as it pertains to cyberspace and ES data.

Collecting ES data is not subject to intelligence oversight laws and regulations unless it is stored or evaluated, in which case it must adhere to intelligence oversight at the point the intelligence begins. In the case of aviation combat element (ACE) units that collect electronic signals and may even display or share the collection for I&W purposes, intelligence oversight is not required until it is stored or evaluated for accuracy or against other intelligence information. Once required, intelligence oversight must begin wherever these actions take place.

Cyberspace activities conducted for intelligence purposes require intelligence oversight. Cyberspace activities conducted for non-intelligence purposes by non-intelligence personnel do not require oversight. Since storing information is one of the two elements that make non-intelligence information into intelligence, and the internet stores information by its nature, information is considered intelligence if it meets either of the following criteria:

- Information collected on a target or adversary automated information system or network by intelligence personnel.
- Information obtained by an automated information system or network enabled for intelligence purposes.

Created to establish a charter for the intelligence community, EO 11905 includes provisions for an intelligence oversight mechanism. Consequently, the SecDef directed the establishment of an Inspector General for Intelligence in the OSD, responsible for the independent oversight of all DOD intelligence activities. The Marine Corps SIGINT community answers this oversight requirement through quarterly reports to the Marine Cryptologic Office. The Marine Cryptologic Office submits their SIGINT oversight reports to the DIRNSA, Headquarters Marine Corps, Office of the Inspector General's intelligence oversight officer, and the DIRINT.
EO 11905 was superseded by EO 12333, and EO 12333 as amended by EOs 13355 and 13470.

Signals Intelligence Oversight Process

DODDs 5148.11 and 5240.1R provide guidance and regulations governing intelligence activities and oversight for all DOD intelligence personnel. These directives also include tasking, collection, processing, exploitation, and dissemination of intelligence.

DODD 5148.11 provides the roles, responsibilities, and authorities of the Assistant to the Secretary of Defense for Intelligence Oversight. Besides overseeing the quarterly and yearly oversight reports, this office conducts yearly audits for the expenditure of intelligence commercial funds (e.g., contractors).

DODD 5240.1R provides guidance for protecting sources and methods for all DOD personnel. It is the responsibility of intelligence personnel to ensure non-intelligence personnel (with a need to know) do not give up these sources and methods. It also provides oversight and policy guidance on sensitive intelligence activities for DOD personnel.

When working with joint, coalition, or host intelligence activities, DOD intelligence professionals must adhere to all USG and DOD rules and regulations. Of particular concern are intelligence and intelligence related activities on the internet, since it is a new area and its activities are not well understood. While much of the information posted on the internet is publicly available, intelligence professionals must have an officially approved mission and tasking before collecting, retaining, or disseminating publicly available information.

For SIGINT personnel, the main intelligence oversight regulation is USSID18, which covers the rules concerning communications to, from, or about US persons and citizens.

The term "US persons" includes US citizens but is broader and includes permanent-resident aliens, unincorporated associations substantially composed of US citizens or permanent-resident aliens, and corporations incorporated in the United States and not directed and controlled by a foreign government.

United States law protects all US persons anywhere in the world, and all persons within the United States, from unreasonable searches and seizures. All electronic signals (e.g., telephonic, web- based, radio transmissions, etc.) used by US citizens are protected by these laws. It is therefore mandatory that SIGINT operations that do or may involve US citizens must be in accordance with the law.

This law aims not to deny or suppress the collection of legitimate foreign intelligence but to ensure the protection of US persons. There are approved procedures implemented when any communications thought to include a US person or transmitted over a US company's media happens in which the foreign intelligence can be exploited while protecting those US persons and companies. Before any US person's communications can knowingly be collected, a warrant must first be obtained from the Foreign Intelligence Surveillance Act court.

Signals Intelligence Oversight Violations

In cases of accidental collection against US persons, Marine Corps SIGINT personnel must ensure all copies of the collection are deleted immediately. Then they must notify the Marine Cryptologic Office of the infraction. Personnel are also required to add these incidents to their quarterly oversight report.

The most important part of accidental collection is ensuring there is no retention or analysis performed on these reports. There are occasions, however, when SIGINT externals are processed and analyzed before knowing that they belong to US persons. Immediately upon realizing this information involves US persons, as with collection, all information (externals and internals) must be destroyed, and the Marine Cryptologic Office notified of the incident.

If for any reason the US person's information has already been released, SIGINT personnel must treat this as a classification spillage and notify the MAGTF Special Security Officer (SSO), who will address the spillage safeguard procedures and report the incident appropriately. Spillage safeguards are handled by the MAGTF G-2/S-2 Systems standing operating procedures (SOPs), G-6/S-6 local SOPs, appropriate DOD regulations, and the DIRNSA's Committee on National Security System's National Instruction on classified information spillage.

Signals Intelligence Releasability

To avoid violations, SIGINT personnel must understand the rules and regulations concerning the release of SIGINT. SIGINT, like all intelligence, must only be released to personnel who have the appropriate clearance level and need to know. The basics of releasability to personnel receiving SIGINT must be cleared, authorized, and a need to know.

Numerous USSIDs relate to SIGINT information handling and releasability. However, these USSIDs are all classified, and no further information can be provided in this document.

SIGINT information is typically classified as Top Secret/Special Intelligence, also called category III information, or Secret/Special Intelligence, also called category II information.

The RadBn OCAC, as the senior SIGINT authority in the MAGTF, is responsible for ensuring proper classification, handling, storage, release, sanitization, and dissemination of all SIGINT information and material.

HOW SIGNALS INTELLIGENCE AUTHORITIES APPLY TO THE MAGTF

These higher-order policies and directives essentially reiterate and implement the same overarching construct—the US SIGINT system must be unified, and the DIRNSA/CHCSS is the authorized agent within the DOD to prescribe SIGINT policy and procedures (SIGINT OPCON). Service SIGINT assets must follow the policies and directives to be part of the USSS, but the DIRNSA/CHCSS is directed to delegate the SIGINT operational tasking of organic assets to the CMC.

The following terms, found throughout the higher-order policies and directives, require further elaboration as they relate to MAGTF operations:

- Signals Intelligence OPCON—the authoritative direction of SIGINT activities, including tasking and allocation of effort, and the authoritative prescription of those uniform techniques and standards by which SIGINT information is collected, processed, and reported. SIGINT OPCON comprises SIGINT Technical Control (TECHCON) and SIGINT Operational Tasking Authority.
- Signals Intelligence TECHCON—the authoritative prescription of those uniform techniques and standards by which information is collected, processed, and reported. NSA derives its TECHCON authority from EO 12333 and DODI O 3115.07. The DIRNSA/CHCSS establishes these techniques and standards through the USSID system. The authority cannot be delegated or in any way divided and include the following points:
  - Through TECHCON, DIRNSA/CHCSS can grant or restrict Service SIGINT assets' use of certain collection; processing; exploitation; and analytic capabilities, techniques, or processes.
  - The decision to grant or restrict is weighted heavily on the compromise of sources and methods, the exposure to compartmented or protected data, and the efficient and effective allocation of USSS resources (to include organic SIGINT capabilities).
  - SOTA is a military commander's authority to operationally direct and levy SIGINT requirements on designated SIGINT resources; includes the authority to deploy and redeploy all or part of the SIGINT resources for which SIGINT operational tasking authority has been delegated. SOTA encompasses the authority to levy tasking on SIGINT resources that collect, process, exploit, analyze, produce, and disseminate SIGINT data, information and/or products.

While the DOD policies direct the DIRNSA/CHCSS to delegate standing SOTA over organic SIGINT units to the CMC, the DIRNSA/CHCSS must approve the SIGINT missions of the SIGINT units, platforms, or other assets assigned to and under OPCON of a military commander. They do this through the USSID systems. A USSID is the DIRNSA/CHCSS approved mission for a SIGINT unit.

The DIRNSA/CHCSS delegates, in writing, standing SOTA for those SIGINT functions and tasks identified in each unit's USSID. In a letter to the CMC in June 2006, the DIRNSA/CHCSS formally delegated standing SOTA to Marine Forces (MARFOR) commanders with organic SIGINT units. At the time, only Marine Forces Pacific (MARFORPAC), Marine Forces Command (MARFORCOM), and MARSOC had organic SIGINT assets. Currently, MARFORPAC, MARFORCOM, MARSOC, and MARFORCYBERCOM have organic SIGINT units with USSIDs approved or in the approval process. The DIRNSA/CHCSS specifically withheld standing SOTA for CNE activities unless those activities are already covered in a unit's USSID or in a functional USSID applicable to the entire USSS.

Marine Corps commanders with designated SIGINT units may further delegate SOTA to subordinate commanders who have tactical SIGINT units assigned to them from one of the USSID-holding SIGINT organizations. Typically, Marine Expeditionary Force (MEF) commanders, Marine Expeditionary Brigade (MEB) commanders, and Marine Expeditionary Unit (MEU) commanders are delegated SOTA over those SIGINT assets assigned to them.

A MAGTF is a composite organization where SIGINT units from multiple MARFORs may assemble to form one unified Marine Corps SIGINT activity in support of the MAGTF. While SOTA may have been delegated to multiple commanders with SIGINT detachments (e.g., one or more MEUs joining a MEB), the senior Marine Corps commander with SOTA prevails. All Marine SIGINT assets fall under the SOTA and the direction of the senior commander.

The senior commander's OCAC implements the MAGTF commander's SOTA. There is only one OCAC in a MAGTF, and it is the commander's SIGINT collection management authority (CMA). The SIGINT CMA operates under USSID authorities and exercises day to day technical control and management functions essential to mission success.

Due to the operational imperatives surrounding the explosion in network connectivity and the advances in technologies to collect, process, exploit, and analyze signals, every echelon mutually supports every other echelon, from tactical to national. Although SIGINT collection teams certainly collect, process, and exploit, they also conduct triage analysis and provide SCI communications to cleared leaders in the supported command. Operations Control Elements (OCEs) and the OCAC provide analysis and reporting but also process and exploit organic and non-organic collection. Even garrison SIGINT units are supporting forward deployed SIGINT elements with processing, exploitation, and analysis.

The USSS is a functioning enterprise where information is pushed, pulled, and shared more rapidly and in greater volumes than ever before. The emphasis in the MAGTF is no longer on collection alone. Instead, it is on a federated SIGINT process where MAGTF analysts can access all raw SIGINT related to the MAGTF's AOI and where MAGTF collection is shared with USSS analysts who may require the signals collected in the MAGTF's AO.

In coordination with military commanders, DIRNSA/CHCSS can manage resource allocation via federated processes through which they effectively delegate temporary SOTA to military commanders to work specific functions. These federated processes are usually specific to collection, processing, and/or exploitation, and details are mission specific and usually classified. Managing the overall SIGINT mission and using temporary SOTA is another way the DIRNSA/ CHCSS can reduce inefficiencies and redundancies throughout the USSS.

Today mission delegation not only includes the standing mission found in the unit's USSID, but it also includes missions the DIRNSA/CHCSS temporarily delegates to units based on concepts of operations, certified personnel, and need to know. Commonly called mission delegation, it addresses access by authorized members of the SPC to national level raw SIGINT databases required to support local commanders. It is called mission delegation because tactical units are theoretically taking parts of a mission performed and managed by national level intelligence personnel. Once the local military mission ends, so does the access to the database.

Safeguarding Signals Intelligence

Safeguarding SIGINT, like all intelligence, is everyone's responsibility. In coordination with MAGTF staff, SIGINT planning and operation personnel provide oversight and ensure compliance with governing policies and directives. Since policies and directives do receive updates, SIGINT units and personnel must stay informed of changes to policies in safeguarding SIGINT information.

Personnel Security Program

The protection of SCI is directly related to the effectiveness of the personnel security program. Intelligence Community Directive (ICD) 704 establishes the personnel security standards for the United States intelligence community. A mutually supporting series of program elements (e.g., need to know, investigation, binding contractual obligations on those granted access, security education and awareness, and individual responsibility) provides reasonable assurances against compromise of SCI by those authorized access to it.

Access Approval Authority

In accordance with ICD 704, the Director of Naval Intelligence is authorized to grant, deny, or revoke SCI access to Marines and Sailors. This responsibility is carried out through the Department of Defense Central Adjudication Facility, which may grant an individual SCI access when the following requirements have been met:

Need to Know is Determined. Even when approved for a specific access, the holder is expected to acquire or disseminate only that SCI essential to carry out an assignment effectively. No person will have a need to know solely by virtue of rank, title, or position.

Eligibility is Determined. ICD 704 provides eligibility standards for investigation and evaluation for an individual's access to SCI. A single scope background investigation conducted within the last five years serves as the basis for determining access approval.

Security Indoctrination is Completed. SCI indoctrination is the instruction an individual receives prior to receiving access to SCI systems, programs, and materials. The instructions convey the unique nature, sensitivity, and special security safeguards and practices for SCI handling, particularly the necessity to protect sensitive sources and methods.

Nondisclosure Agreement is Signed. As a condition of access to SCI, individuals authorized SCI access must sign a DCI authorized nondisclosure agreement (NDA). The NDA establishes explicit obligations on both the Government and the individual for the protection of SCI. An NDA is binding for life and cannot be revoked or waived. Failure to sign an NDA is cause for denial of SCI access.

Physical Security

All SCI must be processed, used, and stored within an accredited sensitive compartmented information facility (SCIF). Accreditation is granted when the proposed facility meets the physical security standards stipulated in ICD 705. The SSO, DIA, is the accreditation authority for all DOD SCIFs, while NSA is the accreditation authority for all Service cryptologic element (SCE) SCIFs. Coordination with the Intelligence Enterprise Management Office (I EMO) is necessary to provide oversight and guidance. Organizations are responsible for ensuring that SCIFs are established only when operationally required and when existing SCIFs are inadequate to support the unit's mission.

Sensitive Compartmented Information Facility. A SCIF is an accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or electronically processed. Access to SCIFs will be controlled to preclude entry by unauthorized personnel. Non SCI indoctrinated personnel entering a SCIF must be continuously escorted by an indoctrinated individual who is familiar with the security procedures of that SCIF. The physical security protection for a SCIF is intended to prevent and detect visual, acoustical, technical, and physical access by unauthorized persons.

Temporary Sensitive Compartmented Information Facility. Recognizing the need for SCIFs to support tactical operations, the Office of the Director of National Intelligence (ODNI) requires the following minimum physical security standards for a temporary sensitive compartmented information facility (TSCIF). The SIGINT unit will provide the measures to meet the requirements to the supported command for coordination and approval of TSCIF operations:

- Locate the TSCIF within the supported headquarter's defensive perimeter, preferably within its main command echelon.
- Use permanent type facilities, if available.
- Maintain 24 hour operation under field or combat conditions.
- Establish a physical barrier around the TSCIF. Where practical, the physical barrier should be triple-strand concertina of general-purpose barbed-tape obstacle. The TSCIF approval authority determines whether proposed security measures provide adequate protection based on local threat conditions.
- Guard the TSCIF perimeter by stationing walking or fixed guards to observe the controlled area. Guards will be armed with weapons and ammunition in accordance with Marine Corps Order 5500.6H w/CH 1, *Arming of Law Enforcement and Security Personnel and the Use of Force*.
- Restrict access to the controlled area with a single gate or entrance that is guarded continuously.
- Maintain an access list. Only those people whose names appear on the list will be allowed access to the TSCIF.
- Staff the TSCIF with sufficient personnel as determined by the on site SSO or G-2/S-2 based on the local threat conditions.
- Keep emergency destruction and evacuation plans current.
- Store SCI material in lockable containers when not in use.
- Establish and maintain communications with local security or emergency reaction forces, if possible.
- Conduct an inspection of the vacated TSCIF area. The SSO or G-2/S-2 ensures SCI materials are not inadvertently left behind when the TSCIF displaces.
- Coordinate planning with the unit's headquarters commandant, who is responsible for providing TSCIF guard personnel, communication with command post guard forces, emergency personnel reaction forces, and internal reaction forces.

If the situation and time permit, these minimum standards will be improved using the security considerations and requirements for permanent secure facilities.

Mobile Temporary Sensitive Compartmented Information Facility. Mobile TSCIF requirements are as follows:

- Maintain a 24 hour operation and staff the TSCIF with sufficient personnel as determined by the on site SSO or G-2/S-2, based on local threat conditions.
- Incorporate external physical security measures into the perimeter defense plans for the immediate area in which the mobile TSCIF is located. (A physical barrier is not required as a prerequisite to establish a mobile TSCIF.)
- Use Marines performing the day to day operations of the TSCIF to control external physical security.
- Establish and maintain communication with backup guard forces, if possible.
- Incorporate incendiary methods in emergency destruction plans to ensure SCI material can be completely destroyed during emergency situations.
- Adhere to the following restrictions when using a rigid-sided shelter or portable van:
  - Mount the shelter to a vehicle so that the shelter can move on short notice.
  - Affix a General Services Administration (GSA) approved security container permanently within the shelter. Protect the lock combination to the level of security of the material stored therein.
  - Control the entrance to the mobile TSCIF with SCI indoctrinated Marines on duty within the shelter.
  - Limit entrance to the mobile TSCIF to SCI indoctrinated personnel.
  - Store classified material within the locked GSA container and secure the shelter's exterior entrance during redeployment.
- Adhere to the following restrictions when using a mobile TSCIF for a soft sided vehicle or man portable system:
  - Protect SCI material in an opaque container (i.e., leather pouch, metal storage box, or other suitable container that prevents unauthorized viewing).
  - Keep this container in the physical possession of an SCI indoctrinated person.
- Limit the quantity of SCI material permitted within the mobile TSCIF to that which is essential to sustain the mission. Employ stringent security arrangements to ensure that the quantity of SCI material is not allowed to accumulate more than is necessary.

Emergency Action Plans. Each accredited SCIF will establish an emergency action plan. This plan will be approved by the appropriate G-2/S-2 or SSO. The essential concern of the plan must be safety of personnel over other factors. The plan will address—

- Physical protection of personnel working in the SCIF.
- Adequacy of firefighting equipment and life support equipment (e.g., oxygen and masks).
- Entrance of emergency personnel (e.g., police, medical technicians, and firefighters) into a SCIF.
- Evacuation plans for persons.

- Emergency destruction and transfer procedures of classified material and equipment in the event of—
  - Fire.
  - Loss of essential utilities.
  - Sabotage.
  - Riots.
  - Civil disorders.
  - Hostile or terrorist attack or capture.
  - Natural disasters.

Temporary Sensitive Compartmented Information Facility Accreditation. The accreditation process consists of three steps, each requiring a message to be sent to the cognizant approval authority (see DODM 5105.21, Vol 1). Approval authorities vary with respect to information and formats required. When requesting TSCIF authorization and accreditation, use the current reference from the cognizant authority. The following reports and messages are prepared by the unit SSO or G-2/S-2:

- Concept of Operations.
  - A message that outlines the who, what, when, where, and why for the TSCIF and identifies supporting security, administrative, and point of contact information.
- TSCIF Activation Report.
  - A report sent to the approval authority upon commencement of TSCIF operations.
- TSCIF Deactivation Report.
  - A report sent to the approval authority when the TSCIF has ceased operations and has been certified to be free of SCI material.

Information Systems Security

All SCIF intelligence and information systems used for processing, storing, and conveying intelligence and SIGINT information must be accredited prior to operating. The I EMO is charged the responsibility for establishing and managing the SCI Information Technology (IT) Enterprise therefore will represent Marine Corps' intelligence as the SCI level IA office. I EMO will coordinate administrative oversight of unit System Security Authorization Agreements and system security plans prior to submission to accrediting agencies. While conducting these duties, the I EMO will collaborate with NSA IA (NSANet) and Naval Intelligence IA (JWICS) on those systems associated with those networks.

The SSO is responsible to the G-2/S-2 for overall management and administration of the unit's SCI security program and SCIF security. The unit's information system security manager and the information system security officer complement the SSO and are accountable for the SCIF resident information systems. The information system security manager or information system security officer will help ensure new and changed information systems meet all security requirements. They will do this with coordination with the I EMO.

Information System Security addresses the integrity of SCI information. It includes protecting against the alteration or destruction of networks, systems, or information. Maintaining integrity requires protection and monitoring in the physical and information domains. Units within the SIGINT and SCI Communications Architectures will work with the I EMO to protect the Enterprise against attacks and will help safeguard the network from vulnerabilities. Ideally, the SIGINT and SCI Communications Architectures will be impervious to threats against its integrity. Practically, it must resist such threats with multiple layers of defense. It must also provide awareness of attacks as they happen so that defensive or remedial measures can be taken. The desired end-state is an enterprise that negates enemy and insider (both intentional and unintentional) threats or, at least, minimizes their effect. Any loss or alteration of information will be remedied via rest oral procedures. Formalized reporting will come from the I EMO.

CHAPTER 4. SIGNALS INTELLIGENCE COMMUNITY

Secure, reliable, and fast information systems architecture is required in order to execute the full range of SIGINT missions. This architecture can be leveraged to receive SIGINT and all source intelligence products and share collected data, products, and reports with the MAGTF, DOD partners, the national SIGINT community, and other national parties.

Since 2001, advancements in information systems technology have led to substantial changes in SIGINT operations. SIGINT architectures that once relied on separate, secure, 24 hour manned communications centers with dedicated, bulk encrypted links now use multilevel information system security initiative capabilities over either unsecured commercial links or DOD networks via the Defense Information Security Agency.

The MCISRE benefits from these changes as it requires all sensor data and other battlefield information to be ready for intake by intelligence processing and analytical systems. As a result, the flow of information moves intelligence data horizontally and vertically throughout the MAGTF, Joint and Coalition forces, and across multiple security domains.

Command and control for SIGINT units and their integration with multi-disciplined intelligence operations requires SCI communications and information systems (CIS). Every mission and situation is unique, requiring some modifications to the information systems architecture supporting SIGINT operations. Detailed planning and close coordination among the Marine Corps' SIGINT community, MAGTF staff, and national IC are critical for establishing a reliable and effective SIGINT architecture.

For more information, see Chapter 6, Planning and Operations.

MARINE CORPS INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE ENTERPRISE

The function, roles, and missions of the Marine Corps SIGINT community are nested under the MCISRE. The goal of the MCISRE is to reduce inefficiencies across the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P) spectrum and deliver timely, relevant, and accurate intelligence to decision-makers at all echelons of command. In other words, the MCISRE aims to eliminate stovepiping in the Marine Corps SIGINT community.

The MCISRE includes the policies, organizations, equipment, processes, and facilities needed to harmonize all service ISR elements into a universal system, networked across all echelons and functions. This Enterprise encompasses the operating forces, supporting establishment, and associated systems and personnel.

The MCISRE roadmap provides the framework and Service-level direction for the continued development of an all source ISR Enterprise that is integrated and used by warfighters across the range of military operations and environments in which Marines may operate.

The MCISRE comprises expeditionary and reachback networks, each providing component elements the ability to contribute or access the awareness, data, resources, and expertise of the entire Enterprise, including national, joint, and combat support agency capabilities. As an integral component of the MCISRE, the Marine Corps SIGINT Community brings its organic capabilities along with the available USSS resources to enrich and expand the scope and all source capabilities of the MCISRE.

UNITED STATES SIGNALS INTELLIGENCE SYSTEM

The United States SIGINT System is a unified organization of SIGINT activities under the direction of the DIRNSA/CHCSS. It consists of the NSA/CSS, components of the military Services authorized to conduct SIGINT, and such other entities (other than the Federal Bureau of Investigation) authorized by the National Security Council or the SecDef to conduct SIGINT activities.

The SIGINT system's success is largely due to NSA's formally established SIGINT OPCON and SIGINT TECHCON over all SIGINT operations, which resulted in developing a coherent architecture for collection, processing, exploitation, analysis, and reporting. Simply put, without the USSS there would be no Marine Corps SIGINT community. The NSA defines membership in the USSS in two ways. The first is as a member of the SCC, and the second is as a member of the SPC.

MARINE CORPS CRYPTOLOGIC COMPONENT

DODD 5100.20, NSA/CSS, defines the SCC as a “term used to designate, separately or collectively, elements of the Army, Navy, Marine Corps, Air Force, and Coast Guard assigned to the CSS by SecDef for the conduct of cryptologic operations funded by NSA/CSS. The commanders of the SCCs represent the interests of their Military Service cryptologic force.” All Services are required to assign an SCC to the NSA to help the national agency accomplish its intelligence mission as defined by DNI. In 2010, the Undersecretary of the Navy established the DIRINT as the chief of the Marine Corps cryptologic component.

Chief, Marine Corps Cryptologic Component

As chief of the Marine Corps cryptologic component, the DIRINT is responsible and accountable to the DIRNSA/CHCSS for all Marine Corps cryptologic matters and ensures Marine Corps compliance with cryptologic policies, tasking, and technical guidance provided by the DIRNSA/CHCSS. The chief of the Marine Corps' cryptologic component meets regularly with the DIRNSA to address operations, policy, budget, training, manpower, and health of the USSS.

Other functions and responsibilities of the chief of the Marine Corps cryptologic component to the DIRNSA/CHCSS include the following:

- Serves as the Marine Corps' voting member of the cryptologic technical advisory group, which sets training and education standards for Service and national SIGINT schools.
- Is responsible for the Marine Corps cryptologic planning, programming, budgeting, and execution, which includes:
  - Providing Marine Corps program objective memorandum (POM) for NSA National Intelligence Program (NIP) and NSA military intelligence program (MIP) funding.
  - Executing current-year Marine Corps NSA NIP and NSA MIP funding.
  - Setting requirements for transitioning NSA developmental technology to Marine Corps SIGINT programs of record (PoRs).

Deputy Commandant for Information (DC I)/Information Intelligence Division (IID). Information Intelligence Division (IID) is responsible for policy, plans, programming, budgets, and staff supervision for intelligence and supporting activities within the Marine Corps. The division supports the CMC in its role as a member of the Joint Chiefs of Staff, represents the Service in Joint and intelligence community matters, and is the functional proponent of Marine Corps intelligence. The DIRINT oversees IID, and as such, chairs the MCISRE operational advisory group and sits at the top of the MCISRE hierarchy, orchestrating the enterprise through policy, direction, and influence.

The division maintains Service staff responsibility for ISR, GEOINT, SIGINT, CI/HUMINT, and measurements and signatures intelligence. It also ensures a single synchronized strategy for developing Marine Corps intelligence, surveillance, and the MCISRE.

The IID also oversees SCI information systems technical architectures and interoperability standards. The division serves as the primary Marine Corps point of contact for plans and policies concerning SCI communications and reviews associated doctrine and policy. Additionally, the division provides and coordinates Marine Corps representation to external committees and working groups addressing intelligence systems technical architectures.

Marine Cryptologic Office. The Marine Cryptologic Office director serves as DIRINT's direct representative to NSA/CSS and provides services supporting all Marine Corps SIGINT entities. The Marine Cryptologic Office coordinates Service and operational issues with the DIRNSA/CHCSS. The Marine Cryptologic Office is the DIRINT's central SIGINT organization and is located at NSA headquarters to perform the following functions:

- Requests delegation of SIGINT authorities to MAGTF commanders.
- Obtains and tracks mission delegation from NSA analysis and production centers to MAGTF and MARSOC elements that are part of the SIGINT production chain.

- Requests clarification and/or modification to current SIGINT policies.
- Manages the intelligence oversight reporting, for MAGTF and MARSOC elements of the SIGINT production chain, to NSA's Office of the Inspector General and HQMC Inspector General.
- Conveys the Marine Corps' needs (policies, capabilities, services) to NSA/CSS.

All Marines planning to visit NSA/CSS, or requiring NSA/CSS support, must coordinate these activities through the Marine Cryptologic Office.

Due to its classification, this document does not include additional Marine Cryptologic Office functions.

Deputy Commandant for Information (DC I)/Information Maneuver Division (IMD). The IMD executes HQMC responsibilities concerning ground EW, SIGINT, cyberspace activities, and intelligence support to Information Operations (IO).

Typical IMD tasks include the following:

- Providing direction and guidance to MARCORSYSCOM SIGINT PoRs and the Radio Battalion Modernization Project for planning, budgeting, and executing NSA MIP RDT&E funding provided through the NSA ISR Portfolio Management Office.
- Representing DIRINT as the voting member on the ISR Portfolio Management Office's TECHCON Advisory Board that approves Services' NSA MIP POM initiatives and current-year spend plans.
- Coordinating with NSA/CSS through the Marine Cryptologic Office to ensure appropriate SIGINT support and technical guidance is provided to Marine Corps operating forces.
- Participating in OSD, Joint Staff, and IC actions concerning SIGINT, EW, cyberspace, and IO.
- Aiding Marine Corps Combat Development Command (MCCDC) in identifying requirements for SIGINT, ground EW, cyberspace, and intelligence support to IO.
- Providing or coordinating Marine Corps representation to external committees and working groups addressing SIGINT, EW, cyberspace, and IO.
- Assisting the Marine Corps SIGINT community regarding research, development, and acquisition initiatives related to SIGINT, EW, cyberspace, IO, and intelligence system technical architectures and standards.
- Serving as the Marine Corps representative to OSD, the Joint Staff, and other DOD agencies for all policy matters involving SIGINT.
- Coordinating with the Director, Marine Cryptologic Office for Service representation to the DIRNSA/CHCSS and the other SCCs.
- Reviewing doctrine and policy that affect SIGINT, ground EW, cyberspace, and intelligence support to IO.
- In coordination with other Marine Corps activities, developing and maintaining applicable cyberspace operations policies that pertain to attack and/or exploitation.

Deputy Commandant for Combat Development and Integration (DC CD&I)/SIGINT occupational field management. The DC CD&I manages the Marine Corps' intelligence personnel structure, career progression, and training.

The DC CD&I/occupational field management tasks include the following:

- Supervising Marine Corps Intelligence career development.
- Coordinating with Manpower and Reserve Affairs (M&RA), MCCDC, Total Force Structure Division, and major subordinate command (MSC) advocates to identify and review intelligence billet requirements for adequacy and applicability to Marine Corps needs.
- Maintaining a central registry of intelligence personnel, including those with an additional MOS 02XX/26XX, to assist staff agencies select qualified personnel for assignment to intelligence billets.
- Advising M&RA when establishing criteria for assignment and voiding MOSs in occupational fields 02/26.
- Coordinating with M&RA on all intelligence MOS manpower issues.
- Monitoring Marine Corps requirements to provide trained intelligence personnel to agencies and commands external to the Marine Corps and the Defense Attaché System.
- Coordinating with M&RA to identify, isolate, and eliminate any intelligence peculiar problems within the Marine Corps force structure.
- Advising M&RA on the acquisition, training, and movement of all occupational fields 02/26 8611 personnel for the Marine Corps.
- Coordinating individual mobilization augmentee (IMA), Selected Marine Corps Reserve units, and Individual Ready Reserve Marines working in support of the DIRINT.
- Assisting in planning for augmentation/mobilization of intelligence reserves in exercise support, special projects, and real world contingencies.
- Coordinating intelligence training and language training input into the training input plan.
- Reviewing all programs of instruction for intelligence courses used to train Marine intelligence personnel and maintaining liaison with Marine Corps representatives at the intelligence schools.
- Reviewing all intelligence publications and training aids for accuracy and pertinence in coordination with the Commanding General, MCCDC, Training & Education Division and Director of Headquarters Support.
- Coordinating with the Deputy Chief of Staff (DC/S) M&RA regarding intelligence personnel sent to intelligence training.
- Serving as the principal interface between the DIA Office of Training, the Director of Naval Intelligence, NSA, and the Marine Corps for all intelligence training matters and the Defense Attaché System.
- Representing the Marine Corps at various training meetings and conferences.
- Maintaining the central registry of foreign language skilled Marines.
- Coordinating with DC/S M&RA on all language skill manpower issues.
- Advising DC/S M&RA on the acquisition of all Marine Corps language training.
- Assisting in planning for augmentation/mobilization of language-skilled Marines in support of exercises, special projects, and real world contingencies.
- Coordinating/managing the Foreign Language Proficiency Requirement Program.

Organization of the Marine Corps Cryptologic Component

The Chief of the Marine Corps Cryptologic Component has control and directive authority over the SCC. The SCC consists of the Commander, MCIA, all MCSB (except Company L), the Marine Cryptologic Office, and parts of the DIRINT's staff established to work SIGINT plans and policies and manage the SIGINT occupational field.

Commanding Officer, Marine Corps Intelligence Activity. The CO, MCIA exercises command and control over the CI/HUMINT Support Company, Production and Analysis Company, and, to a lesser extent, MCSB. DIRNSA retains OPCON of MCSB personnel. The CO, MCIA also exercises administrative and operational control (except SIGINT OPCON) over personnel assigned, attached, or detailed to Cryptologic Services Group (CSG), MCIA.

The CSG, MCIA provides specialized intelligence support to MCIA, including:

- Assisting the CO, MCIA in defining and formulating requirements.
- Assisting in the preparation of support requests.
- Ensuring MCIA receives dedicated on-site, time-sensitive cryptologic support.

The CO, MCIA's authorities and functional responsibilities, as they relate to the Marine Corps Cryptologic Component include:

- Special courts-martial authority over MCSB.
- Responsible to the Commanding General, MCCDC for all Marine Corps directed training requirements.
- Publishes the Marine Corps Mid and Long Range Threat Assessments and Expeditionary Production Requirements, which provide guidance to:
  - Commanding officer, MCSB to plan and coordinate with NSA for short and long term personnel requirements and billet assignments.
  - Commanding officer, MCSB to direct, in concert with the Marine Cryptologic Office and NSA, the Marine Cryptologic Support Elements (MCSEs) operations.

Marine Cryptologic Support Battalion. The MCSB is the SCC force provider to NSA/CSS, under OPCON of the DIRNSA/CHCSS, and provides administrative and logistics support to the SCC. The MCSB trains, employs, and deploys Marines to conduct SIGINT and IA supporting NSA/CSS IRs. The MCSB retains daily operational tasking over the MCSEs, who provide SIGINT "reachback" support, primarily to MAGTFs and other joint forces as directed.

The MCSB is under the administrative control of the CO, MCIA, and consists of a headquarters staff and several letter companies located throughout the United States and overseas. Each letter company provides personnel who integrate into the NSA/CSS missions at their locations. These dispersed units' specific missions are classified, and this document does not include the details.

The commanding officer, MCSB takes direction from the CO, MCIA, and ultimately the DIRINT to negotiate the realignment of Marine billets within the NSA enterprise. Guidance comes in the form of the MCISRE Production Plan and MCIA Threat Assessments. The CO, MCSB, conducts an annual review of Marine billets and recommends changes to the CO, MCIA, and DIRINT. If the changes are approved, the CO, MCSB works with NSA in its POM process to realign billets with Marine focus areas. Short-term realignments may require DIRINT approval since ODNI monitors fill rates for authorized NIP billets.

The MCSEs are subordinate elements of the four letter companies. The MCSEs support NSA's expeditionary SIGINT mission as an NTI gateway between deployed Marine SIGINT units and NSA/CSS. The MCSE provides SIGINT expertise and near real time services via push forward/ reachback capabilities, enhancing USMC components' access to real time, operationally focused, strategic, operational, and tactical intelligence. Due to its classification, this document does not include details of specific functions performed by the MCSE. The DIRNSA/CHCSS delegates daily operational tasking to perform NTI support for deployed forces to the Chief of the Marine Corps Cryptologic Component. The DIRINT delegates the tasking to the CO, MCSB, who provides guidance and direction to the MCSEs.

The mission of the cryptologic augmentation program (CAP) assigned to MCSB is to recruit, screen, join, and retain trained, qualified, and committed IMA Marine reservists. Marines from CAP fill short-term requirements supporting the Marine Corps, DOD, and other US government agencies. The CAP is an IMA reserve unit, not a Selected Marine Corps Reserve unit.

MARINE CORPS SIGNALS INTELLIGENCE COMMUNITY

The Marine Corps SIGINT community is a name used to identify units and personnel who perform or enable SIGINT operations. This community extends beyond the MAGTF and includes support to MARSOC, MARFORCYBERCOM, and the NSA/CSS. The Marine Corps SIGINT community functions as part of two larger enterprises—the MCISRE and the USSS—and has adapted extremely well to significant changes in the communications environment. Marine Corps SIGINT is considered the benchmark of successful tactical SIGINT capabilities. The primary reasons for this success are unity of effort, MAGTF capabilities, and a professionalized workforce.

Unity of Effort

Within the MCISRE, tactical Marine SIGINT supports the MAGTF, focusing on collection, processing, exploitation, analysis, and dissemination. The Marine Corps concentrates tactical Marine SIGINT capabilities at one RadBn per MEF and one MARSOC Marine Raider Support Group. Each of these units organizes tasks in support of ongoing operations and training. Within the USSS supporting establishment, MCSB is task-organized to support NSA/CSS operations worldwide. Smaller and more concentrated than many other occupational fields, the Marine Corps SIGINT community can quickly disseminate and implement organizational changes and new TTPs. Additionally, continuing advancements in high bandwidth communications, common database protocols, and collection and analysis systems allow integration of national and tactical SIGINT operations.

MAGTF Capabilities

The three RadBns and MARSOC Marine Raider Support Group conduct COMINT and ELINT collection and analysis. Fleet Marine Forces neither perform nor require service level training to conduct FISINT analysis.

Professionalized Workforce

Rapid technological developments drove the need for professionalization within the Marine Corps SIGINT community. The community accomplishes professionalization through continual collaboration with NSA/CSS and other DOD elements, including billet assignments and training and curriculum development. The operating forces must maintain a variety of SIGINT systems, both program and non-program of record, to conduct operations. Given the dynamic nature of the operating environment and the rapid development and deployment of improved SIGINT systems, formal entry level SIGINT training provides SIGINT collectors and operators with only a basic level of understanding. Formal follow on training and on the job training are extremely important in developing and maintaining fully qualified SIGINT Marines. Intermediate-level schools, such as the Marine Analysis and Reporting Course, Intermediate Signals Collection Analysis, Intermediate OPELINT, and several progression courses available through National Cryptologic Schools, provide the operating forces opportunities for SIGINT skills training.

In addition to formal follow on schools, career SIGINT Marines rotate between SIGINT operating forces and the SIGINT supporting establishment, professionalizing the Marine SIGINT workforce through exposure to national SIGINT organizations. While assigned to NSA/CSS, Marines are staffed to billets within the NSA/CSS enterprise, where they provide NTI in support of the operating forces, work with emerging technologies, and have access to resident NSA/CSS schools. Both officer and enlisted SIGINT Marines may also apply for one of several multi year cryptologic internships, during which they gain valuable experience and training that they take back to the operating forces.

SIGNALS INTELLIGENCE PRODUCTION CHAIN

The Signals Intelligence Production Chain (SPC) is composed of SIGINT production personnel—collectors, analysts, linguists, reporters, development analysts, staff and support elements, and managers—who produce SIGINT under NSA authorities. As the functional manager of SIGINT, and by virtue of legal authorities granted to it, DIRNSA/CHCSS defines a member of the SPC as “any US Government element assigned a valid SIGINT mission by DIRNSA/CHCSS.” The USSIDs document the approved SIGINT missions maintained by DIRNSA/CHCSS.

Only units with an approved USSID may conduct SIGINT operations, and they do so under authorities delegated from DIRNSA’s Title 50 authorities. Marine Corps organizations under Title 10 authorities may train and educate Marines on SIGINT and equip Marines with SIGINT gear. However, they must be part of the SPC before they may conduct SIGINT operations. Figure 4-1 depicts the SIGINT production chain within the Marine Corps SIGINT enterprise. Marine units within the SPC are the RadBns, MARSOC’s Marine Raider Support Group, and MCSB (with MCSEs providing direct analytic support to MAGTFs).

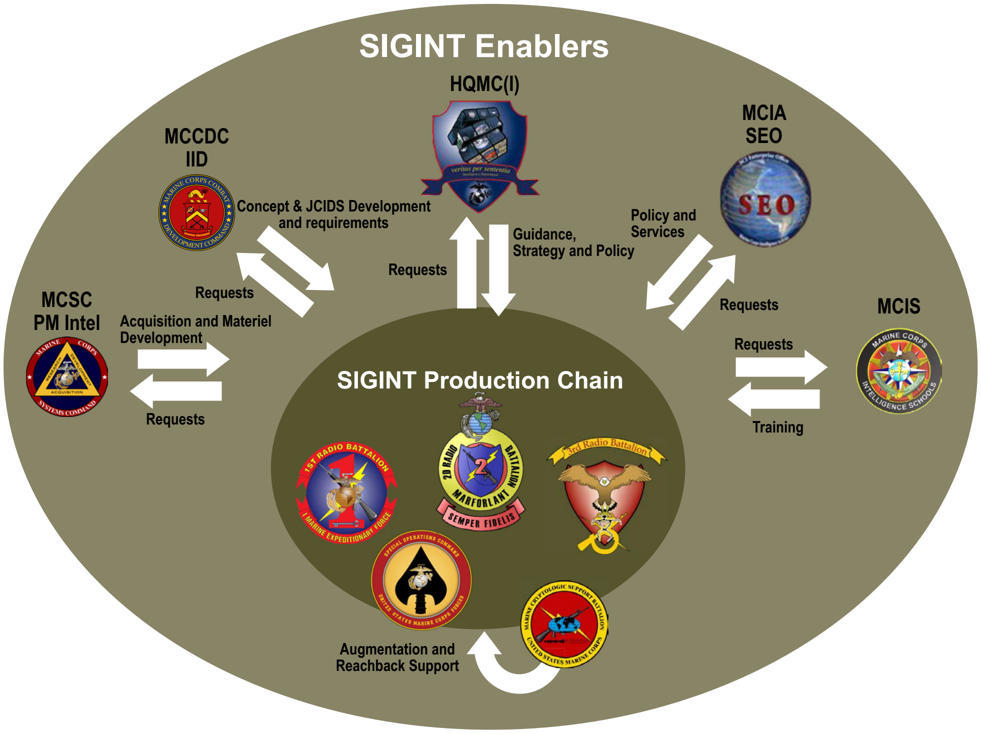


Figure 4-1. Marine Corps Signals Intelligence Enterprise.

FLEET MARINE FORCES

The operating forces contain elements that conduct SIGINT, EW, and limited cyberspace operations with guidance and direction originating at the MARFOR level.

Intelligence Staff Section

The G-2's primary function is to advise and assist the commanding general execute and manage command intelligence, CI, and cryptologic responsibilities.

The G-2 SIGINT/EW branch facilitates SIGINT/EW support to operating forces by:

- Monitoring subordinate SIGINT elements' readiness (e.g., MEF and RadBn).
- Reviewing unit training requirements and mission essential tasks.
- Engaging with Marine Corps Intelligence Schools (MCIS) to enhance and develop effective training for 26XX and 02XX MOSs.
- Reviewing joint and Service SIGINT doctrine and policy.
- Overseeing SIGINT/EW equipment development and fielding.
- Reviewing, assessing, and validating SIGINT/EW-related universal needs statements (UNS) and requirements documents.

Marine Expeditionary Forces

All MEFs and MAGTF intelligence and CI activities, including SIGINT, are under the staff cognizance of the G-2. Within the bounds of the commander's SOTA, the G-2 is responsible for planning, directing, managing, and supervising the tasking and operations of SIGINT units organic to and supporting the MEF.

MEF tasks include the following:

- Develops and satisfies outstanding PIRs and IRs by planning, directing, integrating, and supervising organic SIGINT operations and other MAGTF all source intelligence operations.
- Prepares MAGTF SIGINT plans and orders.
- Coordinates SIGINT collection (to include SIGINT amplifications and SIGINT time-sensitive requirements), production, and dissemination requirements that are beyond the capability of the MAGTF and submits those to higher headquarters for Joint Task Force (JTF), theater, or national SIGINT support.
- Evaluates JTF, theater, and national SIGINT support to the MAGTF and adjusts stated requirements if necessary.
- Identifies, validates, and assists with resolving SIGINT personnel and equipment resource deficiencies (e.g., insufficient linguists or special signal analyst expertise).

Radio Battalions

The MEFs task RadBns to support the MEF and its subordinate elements by conducting:

- SIGINT and EW operations.
- Limited cyberspace operations.
- Special intelligence communications.

Conceptually, the RadBn is a SIGINT, EW, and cyber organization and, therefore, answers to multiple masters. However, at the execution level, RadBn integrates intelligence and operations capabilities in one unit to support the MAGTF mission. It serves predominantly as an intelligence-gathering and analytic organization that increases its effectiveness and capabilities to support the MAGTF when connected and integrated into the larger SIGINT Enterprise. However, there are EW and cyberspace aspects to the RadBns that are not within the intelligence warfighting function and fall under the G-3 instead of the G-2. A RadBn and its detachments deploy in response to the MAGTF's PIRs and IRs, support the MAGTF's targeting priorities, and provide I&W to supported commanders. As a supplemental mission, the battalion and its detachments work closely with the theater and national SIGINT enterprise to answer information requirements and provide access to SOIs.

The three RadBns are—

- 1st Radio Battalion.
  - I MEF Information Group (MIG), I MEF, MARFORPAC.
  - Camp Pendleton, CA.
- 2d Radio Battalion.
  - II MIG, II MEF, MARFORCOM.
  - Camp Lejeune, NC.

- 3rd Radio Battalion.
  - III MIG, III MEF, MARFORPAC.
  - Marine Corps Base Hawaii, Kaneohe Bay, HI.

The RadBn is organized to train and execute operations in general support of the MEF. General support allows the RadBn the freedom of movement and mission tasking necessary to support the MAGTF while providing I&W support to local commanders hosting teams or OCEs. Each RadBn's Table of Organization (T/O) and Table of Equipment (T/E) are based on the MEF's traditional geographic responsibilities, as well as subordinate unit's capabilities and capacities (i.e., light armor reconnaissance, Recon RadBn, etc.).

The RadBn provides support to the MEF and task organizes from within the battalion to source detachments in support of a MEB, MEU, special purpose MAGTF, or other units as directed. The RadBn and its detachments are organized to centrally manage all SIGINT, ground EW, limited cyberspace, and SCI communications operations throughout the MAGTF's AO. The RadBn and its detachments deploy as part of a MAGTF Command Element (CE) unit under the administrative control of the MIG and staff cognizance of the MAGTF G-2/S-2.

Traditionally, a RadBn consists of a battalion headquarters, headquarters and service company, and designated operational companies. The headquarters and service company consists of the staff and support sections and the MEF's operations control and analysis (OCA) platoon. Each operational company consists of a headquarters platoon capable of forming a deployable OCE and SIGINT/EW (SIEW) teams. RadBns may reorganize this structure as required to support each of the MEF's requirements. All RadBn operations, from the OCAC to individual teams, are conducted from sensitive compartmented information facilities (SCIFs). These SCIFs may be permanently fixed facilities or temporary tactical or mobile facilities to support forward-deployed operations.

A RadBn provides one OCAC to support a MAGTF and one or more OCEs at MAGTF MSCs. The OCEs are subordinate to OCACs, can execute tasks and responsibilities delegated from the OCAC, and extend the OCAC's reach throughout the MAGTF AO. The battalion also augments the G-3/S-3 with subject matter experts in EW and cyberspace/cyber network operations.

The OCACs' and OCEs' tasks include the following:

- Collection management for organic and non-organic SIGINT assets.
- Analysis, production, and reporting for SIGINT, EW, and cyberspace exploitation
- Intelligence oversight.
- In coordination with the command G-2/S-2 all source analysts, fusing SIGINT, EW, and cyber with other sources of information.
- In coordination with the G-2/S-2, properly using and handling SIGINT, ES, and cyberspace exploitation.
- Ensuring timely utilization of data across all echelons of the MAGTF while maintaining adherence to US law and DOD policies. For more information, see chapter 3, SIGINT Authorities, Oversight, Tasking, and Control.

The OCAC is responsible for all SIGINT, EW, and cyberspace exploitation activities within the battalion, though it may delegate many functions to lower echelons. The OCAC must maintain oversight and compliance with all laws and policies. The OCAC is the senior SIGINT authority in a Marine AO serving as the battalion's representative to conduct timely SIGINT liaisons with external agencies, including the Marine Cryptologic Office at NSA for policy and authorities. The OCAC is located with the MAGTF's CE intelligence operations center. The OCEs primarily locate with selected combat operations centers within the ground combat element (GCE) and ACE, based on the MAGTF commander's priorities.

The OCE provides the RadBn with extended command and control over SIEW teams and SIGINT operations. The OCEs are task-organized based on the scope of their SIGINT, EW, and cyber functions. The OCE may be manned in a limited capacity to provide only command and control and SCI relay to a supported unit. An OCE, on the other hand, may also be staffed to execute all OCAC functions. An OCE may assume the role of the OCAC in times when the OCAC is displacing or otherwise unable to perform core functions of command and control, threat reporting, or I&W.

The SIEW teams are capable of tactical SIGINT, EW, and limited cyberspace operations, including:

- Survey, collection, and exploitation of enemy signal(s).
    - Including digital networks.
- Geolocation of enemy units.
- Dissemination and utilization of intelligence at the lowest tactical echelons.

A MAGTF commander may disperse SIEW teams throughout the AO, based on the commander's priorities. Access to SOIs is one of the predominant factors affecting the placement of teams within the MAGTF's AO.

Based on the MAGTF concept of operations, the RadBn or its detachment(s) may require specially trained and equipped SIGINT Marines to be formed as one or more radio reconnaissance teams (RRTs) to meet pre-assault, advance force, and/or deep post-assault mission profiles. In these scenarios, the RRT is part of the ground reconnaissance and surveillance (R&S) plan. The team takes its tactical movement direction from the ground reconnaissance commander and its technical SIGINT direction from the RadBn commander. The radio reconnaissance platoon requires similar special insert/extract training, equipment, and certifications required by the division's reconnaissance battalion. For example, per Marine Corps Order 3502.3B, *MEU Special Operations Capable (SOC) Predeployment Training Program (PTP)*, the minimum skills required to be a SIGINT Marine on an Urban R&S team is a 2600 MOS and SOTG Urban R&S Course.

In addition to one or more RRTs, the RadBn or its detachment(s) may include one or more SIEW teams operating from a Light Armored Vehicle (LAV)/EW platform organic to 1st and 2nd RadBns The LAV/EW capability requires those SIEW teams operating from the LAV/EW platform to train and qualify as MOS 0313, LAV Crewman.

The SIEW teams are primarily collection assets that perform low level analysis for I&W purposes. The teams may be further task organized into sub teams for short durations. They may fill a liaison role with battalion or company staffs and provide SCI to cleared commanders and staff; however, this generally takes the team away from collection opportunities. The SIEW teams are best employed as far forward as SOI discovery dictates and may often mean collocation with platoons and squads. The SIEW teams are rarely self sufficient, so they must clearly coordinate logistics, security, and maintenance support arrangements with local commanders before arriving in a local commander's battlespace.

The RadBn also provides the MAGTF a ground non kinetic fires capability via its organic EA systems, supports ACE EW operations with ELINT and sanitized COMINT, and provides limited cyberspace capabilities. The G-3/S-3 tasks RadBn for EW and limited cyber operations, usually through the MAGTF MIG element. The OCAC receives the task and issues fragmentary orders to OCEs or teams directly.

A RadBn, or its detachment(s), will provide organic internal communications, information systems, and SCI communications hardware and keying material necessary to support SIGINT operations. They coordinate bandwidth for SCI circuits with HQMC Expeditionary Warfare Systems and the I EMO, who work with the MARFOR G-2 to acquire SCI circuits.

The RadBns and their detachments require organic communications systems that are properly accredited, secure, flexible, expedient, reliable, and provide continuous terrestrial and/or satellite communications (SATCOM) to subordinate, attached, adjacent, and higher headquarters. The RadBn relies on NSANet for most of its SIGINT operations and must maintain connectivity from the sensors to numerous intra-theater and external theater entities to provide near real time, accurate, and relevant SIGINT and I&W to the MAGTF commander and subordinate elements. The RadBns also leverage NSANet to integrate into the larger theater and national SIGINT Enterprise. Primary communications methods include high-capacity (data rates and bandwidth), low latency terrestrial, or SATCOM at the OCAC, OCEs, and SIEW teams as necessary, and tactical high-bandwidth, low latency terrestrial radios. A RadBn's subordinate elements may require cryptographic keying materials, tactical communication assets, or technical assistance from supported commands to provide immediate threat warning.

A RadBn can perform organic supply functions. When conducting dispersed operations throughout the MAGTF AO, the supported commander may be required to re-supply RadBn elements within their AO. A RadBn, or its detachment(s), possesses sufficient organic motor transport equipment to satisfy routine administrative and operational requirements. However, they may require assistance from the ACE or LCE to support SIGINT and ground EW operations throughout the MAGTF AO.

The RadBn, or its detachment(s), will deploy and employ with general engineering capabilities centrally located with the RadBn CE. General engineering support to dispersed RadBn elements is situation-dependent and may require support from the LCE.

A RadBn is authorized and capable of performing 1st- and 2nd-echelon maintenance of all organic equipment, 3rd-echelon maintenance of all Marine Corps fielded communications/electronic items, and limited 4th-echelon maintenance of Marine Corps fielded SIGINT/EW and special intelligence communications equipment. When conducting dispersed operations, the supported commander may be required to provide 1st- and 2nd-echelon maintenance for RadBn elements within their AO. Theater or national agency-provided equipment may come with stipulations that do not allow local maintenance; the equipment may have to be shipped back to the agency for repair. This must be taken into consideration when planning for equipment maintenance.

Marine Special Operations Command, Marine Raider Support Group

The Marine Raider Support Group trains, equips, structures, and provides specially qualified Marine forces, including operational logistics, intelligence, multipurpose canines, Firepower Control Teams, and communications support to sustain worldwide special operations missions as directed by the Commander, MARSOC.

Marine Corps Forces Cyberspace Command

The MARFORCYBERCOM headquarters consists of a staff with various divisions necessary to function as the US Marine Corps component headquarters for US Cyber Command. MARFORCYBERCOM plans, coordinates, integrates, and synchronizes joint and combined cyberspace requirements enabling freedom of action across all warfighting domains while denying the same to adversarial forces. The MARFORCYBERCOM also directs full-spectrum Marine Corps cyberspace operations, to include DODIN, Defensive Cyber Operations, and, when directed, plans and executes Offensive Cyberspace Operations in support of the MAGTF.

The MARFORCYBERCOM exercises OPCON over Marine Corps Network Operations and Security Center to support mission requirements and tasks. When requested by MARFORCYBERCOM, the Marine Corps Information Operations Center may provide limited network warfare planning support.

The MARFORCYBERCOM coordinates personnel augmentation in support of US Cyber Command joint or combined cyberspace operations. When directed, MARFORCYBERCOM uses specialized cyber staff personnel to perform temporary duties to coordinate operational, training, administrative, and logistical issues when executing Marine Corps tasks.

The MARFORCYBERCOM tasks include the following:

- Comply with US Strategic Command's direction, as stipulated by USCYBERCOM, for operation and defense of the DODIN.
- Integrate the actions of MARFORCYBERCOM's operational forces.
- Synchronize the warfighting effects of MARFORCYBERCOM's operational forces
- In support of USCYBERCOM, plan, coordinate, integrate, synchronize, and conduct activities to direct the operations and defense of the Marine Corps Enterprise Network.
- In support of USCYBERCOM, prepare to, and when directed, attack adversaries in and through cyberspace.
- Operate and maintain a component headquarters collocated with CDRUSCYBERCOM.
- In support of deployed MAGTFs, plan, integrate, and synchronize full-spectrum cyberspace operations.

SUPPORTING ESTABLISHMENT

The remaining elements of the Marine Corps SIGINT community comprise part of the supporting establishment.

Combat Development and Integration, Command Element-Intelligence Division

Command Element Intelligence Division (CE-Intel) integrates, across battlespace functional areas, ISR near-, mid-, and far term requirements to support MAGTF, Joint, and combined operations. As a combat integrator, the Director, CE-Intel, ensures DOTMLPF-P solutions represent a thorough analysis of capabilities needed to provide timely, relevant, and tailored combat information and intelligence to commanders and staff. CE-Intel represents the Marine Corps' intelligence community within the Marine Corps, other Services, and joint forums to which intelligence concepts and requirements pertain.

CE-Intel's tasks include the following:

- Lead the effort to identify MCISRE ISR capabilities necessary to support near-, mid-, and far-term MAGTF operations.
- Coordinate with Capabilities Development Directorate integration divisions, operational users, and others (e.g., DC I IID and IMD, etc.) to include all affected battlespace functions (e.g., fires and maneuver, command and control, etc.) in requirements development for ISR capabilities necessary to support MAGTF operations.
- Validate/non-validate Marine Corps' ISR related UNS.
- Convene and lead integrated planning team in those functional solution analyses necessary to determine DOTMLPF-P solutions for validated UNS.
- Coordinate the development and production of Joint Capabilities Integration and Development System (JCIDS) documentation such as initial capabilities documents, capabilities development documents (CDDs), and capabilities production documents (CPDs) supporting Marine Corps ISR requirements documentation and acquisition programs.
- Accurately represent MAGTF user requirements throughout the acquisition process.
- Adequately assess DOTMLPF-P implications in requirements documents.
- Represent Marine Corps ISR requirements in Marine Corps/joint forums.
- Review and provide comments to other Services and joint ISR initial capabilities documents, CDDs, and CPDs.
- Participate in and provide input to other Combat Development Directorate integration divisions during their respective integrated process teams and, when developing initial capabilities documents, CDDs, and CPDs.

Combat Development and Integration, Command Element Information Warfare Division

Command Element-Information Warfare (CE-IW) division serves as the cyberspace operations division on behalf of DC CD&I. The CE-IW division ensures horizontal integration across all integration divisions and thorough DOTMLPF-P analyses on Marine cyberspace operations.

External to the Marine Corps, CE-IW coordinates with the other Services and the Joint Staff through participation in integrated process teams, Chairman, Joint Chiefs of Staff directed working groups, and responding to staffed draft requirement documents.

Marine Corps Systems Command

The mission of MARCORSYSCOM is to serve as the commandant's agent for acquisition and the sustainment of systems and equipment used to accomplish the Marine Corps' warfighting mission.

Marine Corps Training and Education Command

The mission of TECOM is to develop, coordinate, resource, execute, and evaluate training and education concepts, policies, plans, and programs to prepare Marines to meet the challenges of the present and future operational environments. The command is also responsible for all intelligence-related Marine Corps Reference Publication doctrine.

Marine Corps Intelligence Schools. Marine Corps Intelligence Schools provides functional oversight of all entry level, primary MOS training for (US) intelligence (02XX/26XX) Marines with appropriate minimal security clearances.

Marine Corps Intelligence Schools also provide select intelligence training enhancement and individual skills progression training for intelligence Marines. Through individual skills progression, MCIS provides relevant training solutions directly to the operating forces and assists units with limited “training space” within their PTP timelines.

Twentynine Palms, Tactical Training Exercise Control Group. The tactical training exercise control group conducts Block IV PTP assessment of the MAGTF’s ability to execute core competency combined arms techniques and procedures during full spectrum operations to prepare units for deployment. The tactical training exercise control group also designs, enables, and oversees Service Level Training Exercises for the MAGTF that sustain and evolve live-fire and maneuver combined arms TTPs; simulate combat conditions that improve the rapid decision making cycle; and integrate emergent friendly and threat capabilities in order to improve the MAGTF’s ability to adapt and accomplish missions across the full range of military operations.

MAGTF Tactics and Operations Group. The Marine Corps Tactics and Operations Group provides advanced individual training to designated operations and intelligence personnel within the GCE, provides advanced collective staff training for the GCE, leads GCE doctrine and training standard development and refinement, and examines emerging concepts and technology in order to enhance GCE operational readiness and interoperability in support of the MAGTF.

Marine Corps Logistics Operations Group. The Marine Corps Logistics and Operations Group (MCLOG) manages and runs the Logistics Intelligence Planners Course (LIPC). MCLOG designed this course to advance the understanding of intelligence requirements and intelligence integration with logistics operations across the warfighting functions. Key areas of focus include developing physical network analysis, conducting risk analysis relative to threats in a contested environment, and integrating intelligence collection plans with other elements of the force. LIPC occurs concurrently with the Advanced Expeditionary Logistics Operations Course to drive integration. The target population includes intelligence professionals in logistics units.

Marine Aviation Weapons and Tactics Squadron One. Marine Aviation Weapons and Tactics Squadron One (MAWTS-1) runs two Weapons and Tactics Instructor (WTI) courses per year. WTI is a fully integrated course for highly experienced and fully qualified officers from all aviation communities. Officers from ground combat, combat support, and combat service support also attend the course to ensure appropriate air-ground interface. During WTI, MAWTS-1 conducts several embedded courses, one of which is the Intelligence Officers Course. This course and its integration with WTI serve as valuable training opportunities for SIGINT Marines to learn integration of SIGINT into the overall planning of missions.

CHAPTER 5. SIGNALS INTELLIGENCE COMMUNICATIONS ARCHITECTURE

A component of the SCI communications architecture, the Marine Corps' SIGINT communications architecture provides SIGINT communications services for disseminating SIGINT information. This includes time sensitive and critical SIGINT between the IC and Marine Corps organizations, units, and teams, either garrisoned or deployed. The principal objective of the Marine Corps' SIGINT communications architecture is to provide MAGTF commanders and staffs with information for battlespace awareness supporting the execution of assigned missions.

The SIGINT communications architecture supports this by facilitating the movement of SIGINT data to national support agencies and groups to analyze, produce, and disseminate SIGINT information within the Marine Corps and other DOD and national partners. To accomplish this, the communications architecture must provide an array of voice and data informational services resulting in the timely and reliable dissemination of intelligence information throughout the SIGINT community.

In both garrison and tactical environments, the SIGINT communications architecture consists of a backbone for long haul, high bandwidth communications, Local Area Networks/Wide Area Networks for network connectivity, data dissemination paths for separate communication entry points at the unit and team level, and single-channel radio network for voice communications. The Marine Corps' SIGINT communications architecture is organized around, and managed by, SCI Network Operations Centers (NOCs), located at the fixed site, garrison nodes, and expeditionary nodes, outlined through the MCISRE Roadmap. The SCI NOCs provide operational support, security oversight and compliance monitoring, standardization of policies, procedures, practices, and continuity of operations support.

The SIGINT communications architecture is a net centric operational approach to provide SIGINT data to commanders and throughout the IC by abiding with national policy to ensure the tactical commander can leverage SIGINT information. National-level capabilities, such as the NSANet, JWICS, and SECRET Internet Protocol Router Network (referred to as SIPRNET), enable this access. The operational concept also supports the joint warfighting force by addressing interoperability with joint, allied, and coalition forces to exchange targeting data without exposing collection methods or technologies.

The Marine Corps employs the SIGINT communications architecture across the range of military operations in multiple garrison and expeditionary sites, to include operations afloat. The physical environment ranges from undeveloped/sparsely populated rural areas to highly developed/densely populated urban areas. The terrain includes mountain, desert, and jungle environments with climates (and extreme weather conditions) consistent with the terrain. The operational area may be inhibited or degraded due to friendly, enemy, or neutral force activity and RF spectrum availability. All planning efforts must incorporate communications requirements because these requirements are the backbone of data dissemination from the forward edge to the IC. These plans must include bandwidth requirements, footprint size, and power/cooling considerations.

In support of all communications, the SIGINT communications architecture provides network management and IA. Management provided by this architecture is accessible at all echelons within the SIGINT production chain as a flexible, integrated, and reconfigurable to address changes in requirements. In terms of IA, the SIGINT communications architecture supports secure, accurate, and timely information exchange and provide security that is always available.

Signals Intelligence Support to the MAGTF

The SIGINT communications architecture will provide MAGTF commanders and staffs with timely and accessible information in support of command and control. The MAGTF's SIGINT units must be capable of positive command and control of subordinate units and must integrate their operations with broader MAGTF and external intelligence and operations. Traditionally, single-channel radio and record message traffic were used to support command and control of SIGINT units, but advancements in communications technology expanded the capabilities of other transmission devices. These devices operate at higher data rates and can support file transfer, audio capture/dissemination, electronic email, data-chat communications, and video teleconferencing. The NSANet and JWICS are the Marine Corps' two primary SCI networks.

Secure electronic mail via ultra high frequency (UHF) and high frequency (HF) communications proved to be a reliable means of transmitting doctrinal reporting messages. These same communications assets provide constant connectivity for SIGINT units supporting each echelon of the MAGTF (headquarters to team).

Dissemination

Dissemination is the process through which SIGINT products are delivered to users: the MAGTF commander, subordinate commanders and their staffs, and others as appropriate (e.g., joint force commander, joint components, and various theater and national organizations and intelligence agencies). To disseminate products, SIGINT units use dedicated SIGINT or general purpose channels according to the availability of network resources, the classification of the product, and the intelligence dissemination plan. To the greatest extent possible, it is incumbent on the SIGINT producer to disseminate products within the MAGTF at the lowest possible classification. This requirement usually necessitates at least two versions of any given product: general service (GENSER) and SCI. These products include time sensitive voice reports, text reports, database updates, graphical reports, and data sources (e.g., metadata). Data dissemination occurs using one of several approved mediums capable of making such transfers.

Ability to Provide Intelligence to the Supported Commander

The required SIGINT architecture must support the commander's intent, concepts of operation and intelligence, command relationships, and standing PIRs and IRs. Information gathered from SIGINT must be sanitized or reported via tear line to GENSER channels for further distribution to supported commanders throughout the MAGTF. Cross-Domain equipment or Information

Support Server Environment guards into the network facilitate the movement of traffic or data from multiple networks to support those efforts important to the commander and national allies.

Ability to Receive and Transmit Collected Data and Information

The SIGINT architecture must provide connectivity among organic and supporting SIEW teams, SIGINT analysis and production centers, and supported MAGTF operations and intelligence centers. The SIGINT architecture supports both MAGTF operations within the AO and those missions essential to national interests. Recent years justified the need to directly tie the SIGINT architecture to supported national agencies to facilitate near real time analysis, reporting, and targeting (e.g., real time regional gateway). Requirements include the capability to receive and transmit collection files and reports digitally via fiber, radio (voice and data), or SATCOM, in formats that are readily usable by SIGINT and all source intelligence analysts.

Ability to Share Signals Intelligence Products and Technical Reports, National Audience

The SIGINT architecture must provide the means to share products and reports with MAGTF, theater, and national intelligence centers. The traditional means for providing this capability were the SCI secure Defense Special Security Communication System for record communications and the operator's communications circuit for SIGINT analyst to analyst exchanges and coordination. Over time, direct access to a real time regional gateway campus network, dissemination portals, database access and query tools, and direct analyst to analyst exchanges replaced the previous means by which units and analysts shared products. Though NSANet is the primary system for distributing SIGINT, analysts can also access products on JWICS through a portal. If there is no direct access to NSANet, analysts can reach data through tunneling software. The SCI Network Domain Community consists of the following:

- DIA's JWICS is an SCI NOFORN (not releasable to foreign nationals) network that provides intelligence system interoperability, access to intelligence databases, and direct analyst to analyst exchange. Analysts use the JWICS network primarily to gather all source information.
- NSANet, the backbone of SIGINT production, provides access to national-level SIGINT reports and databases. NSANet connectivity provides SIGINT analysts a medium to exchange electronic mail, use analyst to analyst exchange technologies, and solicit and satisfy intelligence requests.

The Automated Message Handling System allows approved users to query and draft record message traffic from their desktops. This process allows for a larger distribution of formalized traffic (much like the Defense Message System) and simplifies message release. Users can access the Automated Message Handling System on NIPRNET (non-classified internet protocol network), SIPRNET, and SCINET (sensitive, compartmented information network).

Ability to Receive and Disseminate Signals Intelligence Indications and Warnings

A significant strength of SIGINT is its ability to provide time sensitive I&W about the adversary's actions and intentions. Analysts disseminate this I&W intelligence through various means, including voice, record messages, tactical reports, electronic mail, intelligence broadcasts, and chat. Key elements of the SIGINT support provided to the MAGTF include the ability to receive information, recognize I&W intelligence, and disseminate this intelligence to the affected units and decision makers.

Ability to Receive Signals Intelligence Broadcasts

For several years, MAGTFs have been capable of accessing select SIGINT broadcasts using intelligence broadcast receivers. The broadcast receivers currently fielded allow MAGTFs to receive multiple channels of JTF, theater, and national intelligence broadcast data. Intelligence broadcasts occur at scheduled intervals, and requests from commanders and their staffs determine the type of information released. Broadcast information can include all source intelligence, imagery products, recorded briefings, and requested SIGINT data. Operators can provide timely SIGINT support to commanders while preventing information overload through effective planning, designing and integration of SCI and GENSER information systems while employing information management techniques.

Secure Video/Voice Teleconferences

Secure Video Teleconferences (VTCs) are a critical capability within the IC. VTCs facilitate information flow from all echelons of command to support mission and strategic planning. As operational footprints increase, and technology allows, VTCs will become increasingly important for command and control to those outreach areas.

TACTICAL SIGNALS INTELLIGENCE COMMUNICATION EMPLOYMENT

Each Marine Corps' SIGINT element installs and operates SCI terminals for their supporting unit. The MOS 2651, ISR Systems Engineer Marines typically install such systems. They will establish and operate SCI level local area network (LAN) systems to support SIGINT operations. In most cases, Marines deployed to support SCI communications will include communications supervisory personnel, information systems security personnel, system administrators, and communications operators.

Marine Expeditionary Force Support

The MEF SIGINT activities fall under the staff cognizance of the respective G 2s. This includes SIGINT integration into mission planning and product distribution to support operations. For detailed SIGINT support information regarding a specific MEF operation, refer to Annex B of the Operations Order (OPORD) for that operation.

Radio Battalions

Radio battalions primarily operate within the SIGINT environment, can be scaled to fit various MAGTF sizes, and deploy detachments in support of other contingencies. RadBns focus on establishing high bandwidth SCI communication capabilities to push collection, query information, conduct analyst to analyst exchanges, and disseminate intelligence simultaneously. SIGINT elements must prioritize collecting and promulgating raw SIGINT data into the national repository.

Signals Intelligence collection from tactical SIGINT teams is passed to the OCE or OCAC via data and voice over several mediums, including tactical HF, Very High Frequency (VHF), and UHF assets. However, the preferred method for passing collection data is over high bandwidth, small-footprint communication suites, if available. These communication suites should be small enough to support the SIEW team's footprint and easy to operate. Users should also be able to set up and tear down the suites in an expeditious manner.

Marine Expeditionary Units, SIGINT Support Detachment

Marine Corps units aboard US Navy amphibious and/or command ships use the shipboard SCI communications infrastructure while embarked. The Marine unit will provide their own workstations but utilize the Navy shipboard SCI network and transmission systems to connect to the other SCI networks. Once the unit disembarks, it will establish its own SCI/ISR Communication System Architecture.

The method of employment depends on the MEU's mission, threat, and planned concept of operations. The SIGINT detachment is attached to the CE and almost always employed in general support of the MEU. Generally, the MEU SIGINT support detachment, supported by RadBns, consists of an OIC, possibly an assistant OIC, and approximately twenty or more enlisted Marines (to include at least one RRT). The MEU's SIGINT elements deploy differently when afloat and ashore.

Afloat. While afloat, the Marine SIGINT support detachment co-locate in the same facilities as their Navy counterparts. This SCIF, known as the Ship Signal Exploitation Space (SSES), is where both Marines and Navy personnel use SIGINT equipment. Using the ship's communication infrastructure to access JWICS or NSANet can be challenging due to limited bandwidth, but access to the bandwidth can be regulated as needed since the Navy controls all domains through the same device.

In most cases, the SSES gains most of its intelligence data via broadband communications, such as a broadcast service. This type of intelligence "push" is scheduled and can contain vast amounts of data that satisfy the commander's critical IRs. These broadband communications are for inbound traffic only. The SIGINT support detachment must transmit any outbound information through traditional shipboard communications. This means there is a large path for inbound information but only a small path for outbound information. The ship can also receive information from other HF, VHF, UHF, and secure communication links. The amount of data gathered is limited only by equipment capability. Figure 5-1 depicts a secure communications architecture afloat.

LHA/LHD SCI Comm Architecture

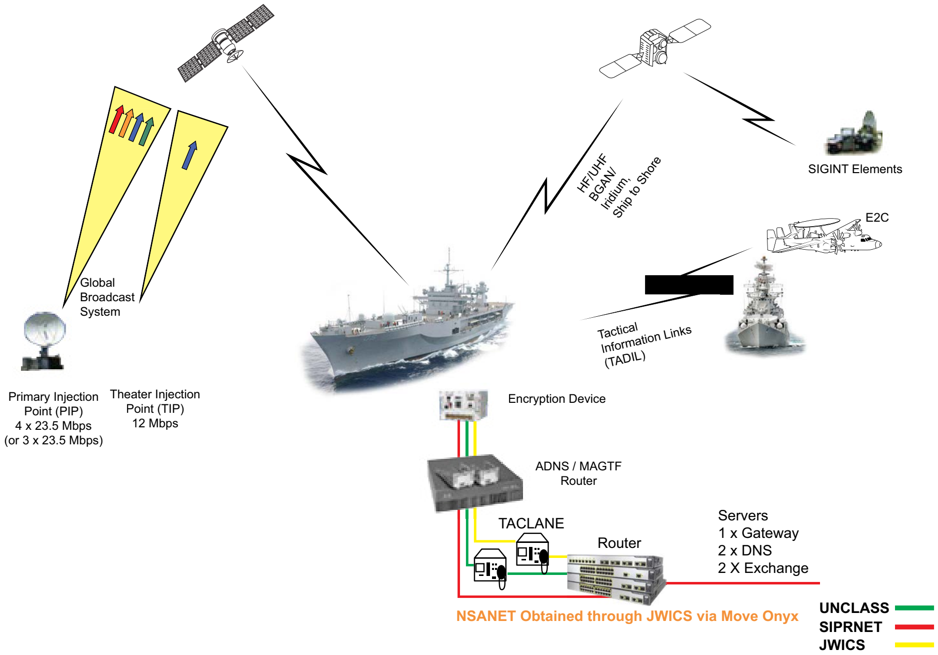


Figure 5-1. Sensitive Compartmented Information Communications Architecture Afloat.

Ashore. The MEU requires ship to shore SCI communications connectivity to continue exploiting external SIGINT capabilities and resources while minimizing the information systems and logistic footprint ashore. The SIGINT operations planning and command and control remain centralized within the MEU S2. Traditionally, a SIGINT element would remain in the SSES to provide additional support to the OCAC. While ashore, however, SIGINT support detachments use the MEU's high bandwidth SCI communication capability rather than depend on the ship's outbound communications. The SIGINT support detachment locates the OCAC with the S2 ashore. Depending on the mission, the SIGINT teams may operate in either general support of the MEU or in direct support of elements operating ashore. SIGINT teams pass tactical SIGINT collection via data and voice over several communication links to both the OCAC and SSES. If available, high bandwidth, small communication suites are the preferred method for passing collected data to the OCAC and national intelligence support agencies because the detachment can stream data as soon as it is collected. Figure 5-2 depicts secure communications architecture ashore.

Marine Special Operational Command

As a service component of United States Special Operations Command (USSOCOM), the commander tasks MARSOC to train, organize, equip, and when directed, deploy task-organized, scalable, and responsive Marine Corps special operations forces worldwide in support of combatant commanders and other agencies. Additionally, USSOCOM tasks MARSOC to conduct foreign internal defense, special reconnaissance, and direct action.

Tactical Reporting Communications Architecture From Ahore

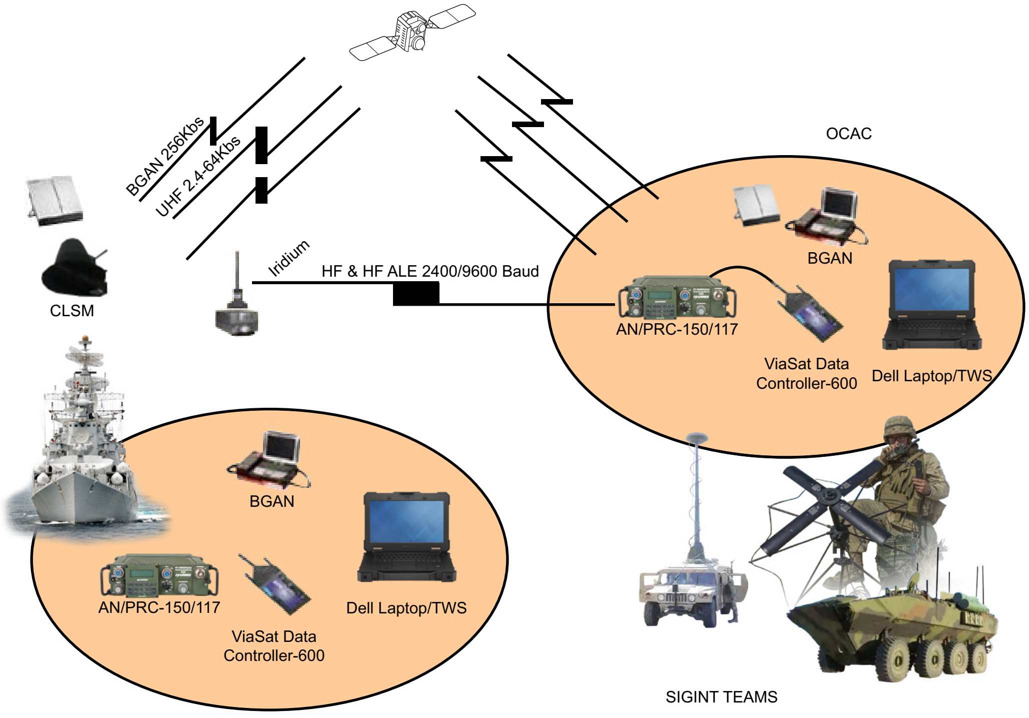


Figure 5-2. Sensitive Compartmented Information Communications Architecture Ashore.

The MARSOC intelligence units operate in a different capacity than RadBns or Intelligence Battalions, but they possess the capabilities of both. Like radio and intelligence battalions, MARSOC intelligence units can access, query, and disseminate large amounts of information throughout the special operations forces community and national intelligence support agencies. Unlike radio and intelligence battalions, MARCORSYSCOM and USSOCOM equip MARSOC.

SUPPORTING ORGANIZATIONS

Sensitive Compartmented Information Enterprise Office

The DIRINT designated MCIA as the executive agent for establishing and managing the Marine Corps I-EMO. The I-EMO advises the DIRINT on SCI IT enterprise plan and policy development and administering that enterprise. The I EMO interacts with SCI systems officers and network administrators across the Marine Corps to provide policy implementation guidance, technical support, and assistance in establishing and sustaining Marine Corps SCI activities.

The I-EMO coordinates strategic and enterprise initiatives, such as providing the support structure to implement SCI NOCs in support of the MCISRE concept. The I-EMO also coordinates initiatives that support joint interoperability and enterprise architectures. Other key functions within the I-EMO are asset management, IT procurement, network engineering, information management, IA, and SCI system/site accreditation in accordance with relevant directives and guidance from the ODNI, Department of Defense Intelligence Information Systems (DODIIS), DIA, and NSA.

United States Navy 10th Fleet

The mission of the 10th Fleet, formerly Naval Network Warfare Command (NNWC), is to “deliver reliable and secure net centric and space warfighting capabilities in support of strategic, operational, and tactical missions across the Navy.” The 10th Fleet is the Department of the Navy’s SCE and directly supports deployed MAGTFs by providing the following:

- Direct service support to MAGTF operations from ashore Navy Information Operations Command facilities in the theater of operations.
- SSES use with MAGTF SIGINT personnel while aboard.
- Direct support to MAGTF operations with NNWC elements operating aboard Navy ships or aircraft.

Certification and accreditation support for sites and systems connecting to the JWICS network, provided by Naval intelligence IA.

CHAPTER 6. PLANNING AND OPERATIONS

The MAGTF's success as the nation's premier, middleweight response force is driven in part by the practice of maneuver warfare through combined arms and mission type orders. The MAGTF's component pieces work together to identify an adversary's critical vulnerabilities, enabling strikes against their center of gravity at the right time and place. Guided by the commander's intent, the component pieces of the MAGTF work together toward commonly understood objectives to accomplish the MAGTF mission. Unlike the rest of the MAGTF, which obtain tasks, constraints, and restraints from the chain of command, the national intelligence community directs MAGTF SIGINT units, and they must adhere to the laws, policies, and directives that govern United States intelligence activities. These intelligence policies affect MAGTF SIGINT activities at all levels, from two person collection teams supporting an infantry squad on a raid to the OCAC located at the MAGTF CE.

Signals Intelligence is a centrally managed enterprise where authorities to conduct SIGINT operations flow to the MAGTF from DIRNSA/CHCSS to the Secretary of the Navy and the CMC. The centralized management and oversight of SIGINT are necessary for several reasons. First, due to its potential intrusiveness and the implications this can have on the privacy of US persons protected under the 4th Amendment, SIGINT is subject to strict regulation by statute and EO. Marines must conduct SIGINT in a manner that minimizes the acquisition, retention, and dissemination of information about US persons, except pursuant to procedures approved by the Attorney General of the United States. Second, SIGINT sources and methods are highly perishable. Therefore, regulations strictly control the protection and handling of SIGINT activities, processes, and information to preserve SIGINT sources and methods.

DIRNSA/CHCSS's authorities over Marine Corps SIGINT capabilities seemingly encroach upon the Service's Title 10 responsibilities to man, train, and equip, as well as the combatant commands' responsibilities to fight wars. The DIRNSA/CHCSS has the authority to prescribe to all Services how to train SIGINT personnel, what equipment SIGINT units may employ (in the conduct of SIGINT), how the Services will conduct SIGINT operations, and when they may do so.

The Services have significant leeway to conduct tactical SIGINT operations with equipment and processes that meet their warfighting requirements. However, over the past ten years, the enterprise saw a requirement for interoperability between globally distributed sensors and processing, exploitation, and analysis nodes, connected by a common network and unified by standardized data formats and analytic techniques. National-to-Tactical Integration was originally a term used to describe the execution of NSA MIP funding for researching and developing interoperable SIGINT technologies and for integrating capabilities across all the Services. It has since become a SIGINT operational concept that defines how the enterprise (processes, capabilities, networks, and functions) mutually supports the warfighter. National-to-Tactical

Integration is becoming the primary means to conduct SIGINT operations. As a result, failure to secure and handle SIGINT data per NSA policies may cause NSA to sever its NTI relationship with offending units, thereby reducing overall support to that MAGTF's mission.

The Marine Corps became the acknowledged leader in tactical SIGINT support to military commanders because commanders and SIGINT professionals follow the rules and regulations issued by NSA/CSS or work with NSA/CSS to modify its policies or procedures. The rule has always been to find innovative ways to work within the system, not find innovative ways to work outside the NSA/CSS system.

There are two primary points derived from this chapter. First, it will serve as a ready guide for non SIGINT personnel to understand the authorities and policies that govern MAGTF SIGINT operations. Second, it will define when the MAGTF must follow SIGINT policies and procedures prescribed by NSA and when the MAGTF has the freedom to conduct signals collection, processing, and exploitation in support of operations that are not subject to SIGINT authorities. When executing EW operations, cyberspace operations, and IO, the clarification of when an activity or information falls under SIGINT authorities is vital.

The balance between support to MAGTF operations and protecting sources and methods is a fine line that SIGINT professionals must walk every day. The goal is to provide SIGINT personnel with clear guidance to allow them to accomplish both. In achieving this balance, the MAGTF will continue to benefit from organic SIGINT assets that leverage the full capabilities of the USSS across the range of military operations.

Signals Intelligence Functional Planning

The principal consideration for planning SIGINT operations (as well as EW and cyberspace operations) is the signal environment. A collection team may require different skill sets depending on the signal environment. In some signal environments, collection teams may require higher capacity communication links to move certain signals around the internal, and possibly external, SIGINT enterprise. In other environments, narrow bandwidth radio links may be sufficient. In many cases, SIGINT's answer to a MAGTF PIRs requirements (also called PIR) may come from an asset located far outside the MAGTF's AO. National capabilities may be required where and when organic assets are not capable against certain signals.

The MAGTF's SIGINT assets exist to support the MAGTF, but organic SIGINT planners must plan for supplemental tasking from NSA/CSS if there is excess SIGINT capacity in the MAGTF. The SIGINT planners must also plan ground EW support and cyberspace enabling operations because the SIGINT collection teams, OCEs, and the OCAC must also conduct EW tasks and specific, but limited, cyberspace operations.

Ideally, the signal environment should drive the allocation of SIGINT resources, not the array of friendly combat forces in the battlespace. To obtain optimal collection, including geolocation, SIGINT equipment and personnel should be located with ground combat elements according to

SOI activity. In an operation ashore where the MAGTF has fixed bases, friendly SIGINT capabilities constantly improve their capabilities and processes to exploit the signal environment. In forcible entry operations where the MAGTF is on the move fighting for battlespace (e.g., the 1991 Gulf War, Operation Iraqi Freedom, and amphibious operations), MAGTF SIGINT assets are usually mobile, which makes it harder for SIGINT Marines to develop targets and prioritize SOIs.

Detailed planning must precede SIGINT operations to identify and exploit the signal environment. The earlier a MAGTF can employ SIGINT survey and collection teams, the better success the MAGTF will have in developing the SIGINT operational environment and producing timely, relevant, and accurate SIGINT. The SIGINT operational environment includes the signal environment and the USSS capabilities arrayed against the AO and AOI. While the AO in the SIGINT operational environment remains a geographic area with defined boundaries, the AOI is potentially global and defined logically by the signals relevant to the MAGTF's mission in an AO. The MAGTF must employ collection and analytic efforts at the right place (physically and technologically) and in time to ensure that SIGINT operations are optimized to support its concept of operations.

SIGNALS INTELLIGENCE CONCEPT OF OPERATIONS

The following questions must be answered to develop the SIGINT concept of operations:

- What is the MAGTF AO, AOR, and AOI?
- What are the MAGTF concept of operations, task organization, and main and supporting efforts?
- Does the friendly concept of operations allow for fixed site and mobile SIGINT collection and geolocation operations?
- What are the standing PIRs and IRs? Which have been tasked to SIGINT units? What specific information is the commander most interested in (e.g., enemy air operations, enemy ground operations, friendly force protection, target battle damage assessment, or enemy future intentions)?
- What is the MAGTF force protection concept of operations? The IO concept of operations? The EW concept of operations? The offensive cyber concept of operations?
- What is the MAGTF concept of fire support?
- How will MAGTF target development and target intelligence be conducted?
- What are the SIGINT and intelligence concepts of operations of other JTF components, the JTF, and theater resources?
- What are the task organization and command or support relationships for all other MAGTF intelligence and reconnaissance units?
- How can JTF, theater, and national SIGINT assets be integrated and employed to support MAGTF operations?
- How is the USSS postured, or arrayed, against the MAGTF's AO and AI?

- Which SIGINT operations must be deconflicted, and what is the theater process and national process?
- Are reporting and sharing policies established for the specific AO and the members of the coalition?
- Does the MAGTF have mission delegation to access relevant national databases for the AO and AI?
- Are all signal collection, processing, and exploitation capabilities available to the MAGTF coordinated and deconflicted between the G-2/S-2 and the G-3/S-3?

In major combat operations, the enemy is the number-one focus. However, not all intelligence operations focus on the enemy. In certain operations, intelligence focuses on the population, key leaders, and positive and negative influences on the battlespace's security, governance, and economics.

Size and Composition of Adversary Forces and Enablers

- What threat forces are within the MAGTF AO and AI?
- What are the enemy’s centers of gravity and critical vulnerabilities?
- Is this a large enemy force organized along conventional military lines or small, loosely knit guerrilla’s or irregular non-state military force?
- Who are the high value individuals? Adversary leaders? Enablers? Key leaders within the population? Key enablers within the populations friendly, neutral and threat networks?

Enemy Command and Control, Supporting Communications, and Information Technology

- What and where are the enemy’s critical C2 nodes, and what are their vulnerabilities?
- What types and categories of communications nets and networks does the enemy use?
- What echelons of command do the communications nets and networks serve?
- What are the associated communications and non-communications emitters?
- What are the TTPs used for enemy Computer Information Systems operations? How do they relate to various threat functional activities?
- How is information transferred among the enemy’s units and command echelons?
- Does the enemy employ communications emitters at all levels of command, or does the enemy rely on communications means less exploitable by SIGINT (e.g., fiber, wire, and messenger)?

Irregular Warfare, Crisis, Prolonged Operations Ashore

- What communication technologies do non-state threat groups/networks and individuals employ? Do friendly and netural individuals and groups/networks use electronic communications to perform government (including military) or commercial business, or networking (social, command and control, etc.)?
- What are the demographics of the AOI? Technology distribution (i.e., what communication types are used where, and by whom?) Population density (racially and ethnically)? Age distribution and age of adulthood? Education and literacy rate? Employment rate? Languages and dialects (percentages and distribution)?

- What are the values and beliefs of the different groups in the AOI? Core values and ideals? Where do the values and ideals come from? What is each group’s history? How does each group view and value the others in the AOI?
- Who are the noteworthy groups and individuals in the government? Who are the noteworthy groups and individuals not part of the government? What are the relationships among the groups and individuals?
- What does it mean to be a member of a group? Are their networks or sub-groups among the groups? What are the organizational structures, interactions, and responsibilities of a group?
- How does the populace feel about the United States and US allies? North Atlantic Treaty Organization? United Nations? How does the populace feel about their own government(s)?

For more information about irregular warfare and methods to engage friendly, netural and counter non-state threat networks, see MCTP 3-02A, *MAGTF Network Engagement Activities*.

SIGINT Computer Information Systems and Architecture Planning Requirements

- Add the MAGTF CE, RadBn, and other MAGTF elements to appropriate addressee indicator groups to receive pertinent JTF, theater, and national intelligence and SIGINT products.
- Obtain and activate SCI plain language addresses for MAGTF CE, RadBn, and other MAGTF elements as appropriate. Determine and coordinate wire communications, including telephones.
- Determine and coordinate SCI and GENSER LANs and wide area networks and unique intelligence networks information systems requirements (e.g., hardware, software, internet protocol addresses).
- Determine and coordinate SCI courier requirements and operations.
- Integrate RadBn elements operations with those of other MAGTF and pertinent JTF and other components’ intelligence and reconnaissance units (e.g., mutual support, cueing).
- Coordinate SIGINT CIS and dissemination operations and procedures with allied and coalition forces.
- Coordinate SCI and SIGINT CIS activation and restoration priorities and procedures.
- Determine unique COMSEC material system requirements for SIGINT and SCI communications.
- Determine communications requirements between temporary SCIF (TSCIFs) and mobile SCIFs and supporting security forces.
- Determine and coordinate radio nets, supporting frequencies, and procedures for:
  - MAGTF external SIGINT operations.
  - MAGTF internal SIGINT operations.
  - Intelligence broadcasts.
  - Retransmission sites.
  - Routine and time-sensitive operations.
  - Obtain authority and establish procedures for the sanitization of SIGINT products, reports, and other information.

Security of Sensitive Compartmented Information

Sensitive compartmented information is classified information concerning, or derived from, intelligence sources, methods, or analytical processes and must be handled within formal access control systems established by the ODNI. Only intelligence and information that clearly warrant extraordinary security measures will be restricted to SCI control.

When dealing with issues involving SCI security, refer to the following publications for policy and instructions:

- DODM 5105.21, Vol 1, *SCI Administrative Security Manual: Administration of Information and Information Systems Security*.
- DODM 5200.01, Vol 3, *DOD Information Security Program: Overview, Classification, and Declassification*.
- ICD 503, *Intelligence Community Information Technology Systems Security Risk Management*.
- ICD 703, *Protection Classified National Intelligence, Including Sensitive Compartmented Information*.
- ICD 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information*.
- ICD 705, *Sensitive Compartmented Information Facilities*.
- SECNAVINST 5510.30C, *Department of the Navy Personnel Security Program*.

These documents provide policy and guidance on:

- SCI personnel and information security clearance procedures.
- SCIF and TSCIF requirements.
- Classification levels.
- Compartmentation.
- Decompartmentation.
- Sanitization.
- Release to foreign governments.
- Emergency use.

Security policy and procedures exist to protect information controlled in SCI compartments. Safeguarding SCI is critical as it protects, not only a piece of intelligence, but also its source. For these reasons, dissemination and access to SCI information and materials are restricted. However, to be worthwhile, SCI must be accessible to commanders for use in decision making. SCI must be classified only to the degree necessary in the interests of security. SCI security must be applied within the context of the mission, with security needs constantly assessed and balanced against operational mission needs.

The commander is responsible for SCI security. The commander exercises this responsibility through the unit G-2/S-2. The Special Security Officer (SSO) serves as the primary staff officer for day to day SCI security administration and management. The commander must ensure SCI is accessed only by those with the necessary clearance, access approval, identified need to know, and appropriate SCI indoctrination. This safeguard is accomplished by carefully managing those units and individuals with SCI access and the equipment and facilities used to process, disseminate, and store SCI.

EMITTER TECHNICAL DATA

Effective SIGINT operations require certain technical knowledge of the enemy's communications methods. To acquire this knowledge, analysts may require spectrum, signal, or network surveys. A spectrum survey is a search of the EMS to determine what frequencies are active. A signal survey identifies the type of active technology on a given frequency or set of frequencies. A network survey identifies the technical details necessary to exploit a technology.

BILLETS AND RESPONSIBILITIES

The MAGTF Commander

The MAGTF commander is ultimately responsible for planning and conducting MAGTF SIGINT operations. The MAGTF commander's staff, MSCs, specialized units, and theater- or national-level organizations assist the commander in executing SIGINT responsibilities. This chapter focuses on the SIGINT roles and responsibilities of Marine operating forces' staffs, MSCs, and specialized units.

The MAGTF commanders are responsible for using their organic SIGINT assets effectively and legally and ensuring responsive national and theater support to subordinate commands. MAGTF commanders—

- Review and validate SIGINT support requests from subordinate commands and ensure they receive the tailored support they require.
- Coordinate SIGINT issues and requirements with the JTF commander and combatant commander.
- Coordinate with theater and national SIGINT and all source intelligence agencies and organizations to support the MARFOR.
- Exercise organic SIGINT capabilities, including leveraging theater and national SIGINT capabilities to support the MARFOR.
- Coordinate between MARFOR and their subordinate commands to improve SIGINT interoperability, standardization, preparedness, and performance.
- Delegate temporary SOTA for exercises and operations to MAGTF commanders with organic SIGINT capabilities, and notify the DIRNSA/CHCSS.
- Ensure the proper handling of SCI material and processes and the protection of SIGINT sources and methods.
- Are responsible for the MARFOR's intelligence oversight.
- Provide guidance for MAGTF intelligence center (MIC) operations.

The MAGTF Staff Sections

Primary staff responsibility for SIGINT operations planning lies with the G-2/S-2 whose responsibilities include the following:

- Develop and satisfy outstanding PIRs and IRs by planning, directing, integrating, and supervising organic SIGINT operations and other MAGTF all source intelligence operations.

- Prepare MAGTF SIGINT plans and orders.
- Coordinate SIGINT collection, production, and dissemination requirements that are beyond the capability of the MAGTF and submits them to higher headquarters for JTF, theater, or national SIGINT support.
- Ensure routine and time-sensitive SIGINT information is rapidly processed, analyzed, and incorporated in all source intelligence products and rapidly disseminates this information to MAGTF and external units.
- Evaluate JTF, theater, and national SIGINT support to the MAGTF and adjusts stated requirements if necessary.
- Identify, validate, and assist with resolving SIGINT personnel and equipment resources deficiencies (e.g., insufficient linguists and special signal analyst expertise).
- Incorporate SIGINT in training exercises to improve MAGTF individual, collective, and unit readiness.
- Prepare integrated, multidiscipline intelligence and reconnaissance operations, to include supporting SIGINT plans, orders, annexes, and appendices.
- Coordinate with the G-3/S-3 to ensure planned SIGINT effort will support the concept of operations and scheme of maneuver.
- Coordinate with the G-3/S-3 to ensure SIGINT operations are integrated and deconflicted with the IO, EW, and cyberspace concept of operations.
- Coordinate with the G-3/S-3 to ensure MSCs support adequate site placement and security for SIGINT collection elements operating in their battlespace.
- Coordinate with the G-6/S-6 officer for tactical SATCOM, radio line-of-site, and wireless communications support to SIGINT elements distributed throughout the MAGTF's battlespace, including circuits and networks access, frequency assignment, equipment, and call signs.
- Coordinate with the Marine Corps I EMO for SCI Communications circuits not provided by the G-6/S-6 (i.e., JWICS, and NSANet).
- Act as the senior intelligence officer to external agencies for requirements and feedback to external SIGINT agencies.
- Coordinate with the G-4/S-4 to ensure adequate logistics support for SIGINT elements (e.g., transportation and maintenance of SIGINT units' unique equipment).
- Ensure IO, EW, and Cyberspace IRs are prioritized and answered based on the MAGTF commander's guidance and direction.
- Ensure SIGINT is supporting IO.
- Provide direction for MIC operations.

Primary staff responsibility for IO, EW, and cyberspace operations lies with the G-3/S-3. Because of the close relationship of SIGINT to effective EW and cyberspace operations, the G-3/S-3 has responsibilities for the following:

- Planning and directing geolocation.
- Planning and directing offensive cyberspace missions.
- Planning and directing EW missions.
- Planning and directing IO.

Intelligence Section

Intelligence Operations Officer. The Intelligence Operations Officer (IOO) is responsible to the G-2/S-2 for overall planning and executing MAGTF all source intelligence operations. The IOO—Plans and implements a concept of intelligence operations based on the mission threat, commander's intent, and concept of operations.

- Develops, consolidates, validates, and prioritizes recommended PIRs and IRs to support MAGTF planning and operations.
- Plans, develops, and directs MAGTF intelligence collections, production, and dissemination plans, including effectively employing and integrating MAGTF multi discipline intelligence and reconnaissance operations.
- Coordinates and integrates MAGTF intelligence operations with other components, JTF, theater, and national intelligence operations.
- Evaluates and improves MAGTF intelligence operations.
- Oversees MIC operations.

Signals Intelligence Officer. The Signals Intelligence Officer (SIO) is responsible to the MAGTF G-2/S-2 for planning, directing, and executing MAGTF SIGINT operations. The SIO—

- Coordinates with other intelligence section staff officers, the RadBn CO or OIC, and the ACE G-2/S-2 (for ELINT operations) to prepare SIGINT plans and orders for the MAGTF.
- Coordinates with the collection management officer and RadBn and ACE ELINT planners to coordinate, plan, supervise, and assist SIGINT collection requirements and tasking for MAGTF operations.
- Coordinates with the ground reconnaissance coordinator, the RadBn CO or OIC, ACE ELINT representative, and G-3/S-3 for the movement, operation, and reporting of SIGINT units.
- Coordinates with the MAGTF intelligence operations center (IOC) senior analyst, the OCAC senior analyst, and the ACE ELINT senior analyst to establish analyst exchanges and ensure SIGINT integration with all-source intelligence production.
- Coordinates with the dissemination officer to plan for the timely reporting of SIGINT derived intelligence to MAGTF and external elements and the rapid handling of perishable SIGINT information.
- Coordinates with the G-6/S-6, the G-2/S-2 Systems Officer, GCE G-2/S-2, ACE G-2/S-2, and SIGINT unit OICs to plan and coordinate SCI communications paths and operations.
- Assists the IOO in preparing and presenting SIGINT briefings and reports, as required.
- Oversees the SIGINT portion of the MIC.

Collections Management Officer. The collections management officer (CMO) is responsible for formulating detailed intelligence collection requirements (ICRs) and tasking and coordinating internal and external collection operations to satisfy these requirements. The CMO receives PIRs and IRs from the IOO and develops an integrated collection plan using organic and supporting resources. In coordination with the SIGINT officer and SIGINT unit COs or OICs, the CMO determines and coordinates ICRs that may be tasked to organic or supporting SIGINT elements.

In coordination with the RadBn's OCAC OIC, the CMO identifies ICRs and prepares requests for intelligence that are beyond organic capabilities and must be submitted to higher headquarters and external agencies for satisfaction.

The MAGTF Intelligence Operations Center Senior Analyst. The MAGTF IOC Senior Analyst is primarily responsible for managing and supervising the MAGTF's all source intelligence production and processing effort. The MAGTF intelligence operations center senior analyst—

- Determines and coordinates MAGTF IRs, to include SIGINT element products as well as all source intelligence products.
- Maintains all source automated intelligence databases, files, workbooks, country studies, planning imagery, mapping and topographic resources, and other references.
- Administers, operates, and maintains intelligence processing and production systems, both GENSER and SCI (e.g., joint deployable intelligence support system and intelligence analysis system).
- Analyzes and fuses all source intelligence into tailored products in response to stated or anticipated PIRs and IRs, to include sanitized SCI products.
- Develops and maintains current and future intelligence situational, threat and environmental assessments, and target intelligence.
- Provide all source analyst to analyst exchange with the OCAC senior analyst to ensure SIGINT collaboration and integration with intelligence priorities.

Radio Battalion Commanding Officer or Officer in Charge. The RadBn CO or OIC is responsible for executing SIGINT operations in support of the commander's intent and the operational and intelligence concept of operations. The RadBn CO or OIC:

- Plans and employs SIGINT resources in response to the commander's intent, threat situation, MAGTF G-2/S-2's guidance and direction, and the intelligence operations plan.
- Influences technical direction and control of MAGTF organic SIGINT collection, processing and exploitation, production, and dissemination operations. Also helps coordinate MAGTF SIGINT operations with JTF, theater, national, and other Service SIGINT agencies.
- Establishes the OCAC as the senior SIGINT analytic and production authority and SIGINT CMA in the MAGTF battlespace. Coordinates with the theater NSA/CSS representative (NCR) to recognize the OCAC as the equivalent of NSA's CSG.
- Publishes SIGINT reporting policy and guidance (RP&G) that maintains the MAGTF's SIGINT dissemination rules and reporting formats.
- Coordinates movement and operations of SIGINT units with MAGTF staff elements and subordinate unit commanders. Ensures that all element movements are coordinated with the COC, fire support coordination center, and the IOO.
- Advises the G-2/S-2, SIO, IOO, and the CMO on SIGINT employment and its integration with JTF, theater, and national SIGINT operations.
- Plans and employs EW and cyberspace resources in response to the commander's intent, threat situation, MAGTF G-3/S-3's guidance and direction, and the fire support plan. Deconflicts all EW and cyberspace operations with the G-2/S-2 and the appropriate deconfliction authority in theater.

COORDINATING SIGNALS INTELLIGENCE OPERATIONS

Signals Intelligence operations are coordinated internally within the MAGTF and externally with higher headquarters, national agencies, and adjacent units and agencies.

Internal Coordination

The intelligence staff must coordinate internal MAGTF SIGINT requirements with maneuver, fires, EW, force protection, and cyberspace requirements. This coordination may occur within the cyber coordination cell and the FSCC under the G-3/S-3, within the MAGTF combat operations center, or within the OCAC, depending upon the task organization, command and control, and support relationships in effect. Additionally, the intelligence staff must coordinate collection and geolocation team movements and locations with the MAGTF's concepts of maneuver and fires to ensure continuous support to the main effort without interference. Planning and close coordination must occur among the following MAGTF staff officers:

- MAGTF G-2/S-2, the IOO, and the intelligence battalion commander.
- SIO, MAGTF IOOs, and the collections officer.
- MAGTF G-3/S-3 future and current operations officers, information operations officer, electromagnetic warfare officer, and cyber planners.
- MAGTF G-6/S-6.
- GCE, ACE, and LCE staff officers.
- RadBn Operations and ACE EW shop.

External Coordination

Higher Headquarters and External Organizations. The MAGTF G-2/S-2, via the OCAC operations section, must coordinate SIGINT operations, activities, and requirements with theater and national SIGINT planners and collection and mission managers. In particular, the DIRNSA/CHCSS provides an NCR to the theater to support the JTF's operations and establish DIRNSA/CHCSS authorities over the theater SIGINT operations. Accordingly, a continuous exchange of data and information is required, necessitating NSANet access to exchange SIGINT technical data and intelligence information.

The Marine Cryptologic Office is the primary coordination point for the conduct of SIGINT abroad. Mission planning must include working with them to ensure USSIDs and accesses are appropriate to the assigned mission requirements.

Adjacent Area Signals Intelligence Activities. The MAGTF must coordinate its SIGINT activities with other units conducting SIGINT within the joint operations area and theater to reduce duplication and ensure maximum use of available assets and mutual support. For example, an army unit operating outside the MAGTF's battlespace could be conducting SIGINT collection and geolocation against targets within the MAGTF's battlespace. This may be due to environmental factors affecting RF propagation or the transmission path of the signal. With proper planning and coordination, external SIGINT assets belonging to the combatant commander, JTF, and other components can provide SIGINT support to the MAGTF (e.g., product reporting, exchanging technical information), allowing organic MAGTF SIGINT resources to focus on more critical targets.

If neither a deconfliction agency nor centralized management of SIGINT resources (as well as EW and cyber) exists, the external Joint unit may obstruct MAGTF SIGINT operations. Similarly, organic MAGTF SIGINT operations may interfere with the Joint operations. Depending on local requirements, the MAGTF performs SIGINT operational coordination directly with adjacent units or higher headquarters.

SIGNALS INTELLIGENCE OPERATIONS PLANNING

This section provides a general description of the SIGINT planning process and accompanying activities. This section does not discuss technical details about SIGINT processing. The SIGINT cycle aligns with the six phases of the intelligence process.

For additional information on the intelligence process, see or MCWP 2-10, *Intelligence Operations*, or Joint Publication (JP) 2-0.

Signals Intelligence Planning and Direction

The planning and direction phase of the intelligence process consists of those activities that identify and prioritize pertinent IRs and provide the means to satisfy them. Intelligence planning and direction are continuous functions and a command responsibility. The commander directs the intelligence effort, and the intelligence officer manages this effort based upon the commander's intent, the commander's PIRs, and specific guidance provided during the planning process.

The intelligence planning and direction functions are:

- Requirements development.
- Requirements management.
- Collections management.
- Production management.
- Dissemination management.
- Intelligence support structure.
- Supervision of the intelligence effort.

Signals Intelligence planning is conducted concurrently with overall intelligence planning. It consists of those activities that identify pertinent IRs, are tasked to SIGINT units, and then provide the means for satisfying those IRs. Signals Intelligence planning and direction are continuous functions requiring close interaction between the G-2/S-2 and SIGINT unit planners.

Signals Intelligence planning and direction objectives include:

- Identifying IRs tasked to SIGINT elements.
- Preparing a SIGINT operations plan, to include integral SIGINT collection, production, and dissemination plans.

- Planning and establishing the SIGINT support system (e.g., communications architecture, logistics).
- Issuing orders and tasking to SIGINT units.
- Supervising and coordinating SIGINT operations.

A planner must develop an effective, dynamic SIGINT operations plan to maximize the effectiveness of the SIGINT effort. With the multitude of threat signals on the modern battlefield, whether urban or countryside, the planner must carefully construct the collection plan to collect and exploit enemy signals that are most likely to provide the necessary intelligence data. Additionally, SIGINT production and dissemination plans must effectively support unique SIGINT and all source intelligence operations requirements and operations.

Mission Planning

Based on the commander's PIRs and IRs, the G-2/S-2 determines the ICRs that apply to, and have the potential to be satisfied by, the organic SIGINT collection effort. The G-2/S-2 incorporates these ICRs into the overall intelligence collection plan and issues mission tasking and guidance to the RadBn detachment OIC. The RadBn OIC typically delegates these to the OCAC collection manager or OCAC OIC.

The RadBn CO, or OIC, may need to consider EW and/or cyber tasks from the G-3/S-3 when developing estimates of support and concepts of operation. Additionally, SIGINT, EW, and/or cyber tasking may come from the joint force commander and supplemental tasking (SIGINT) from DIRNSA. The RadBn CO, or OIC, and their OCAC will need to consider all specified and implied tasks for SIGINT, EW, and cyber.

For additional information regarding DIRNSA supplemental tasking authority see USSID 4.

Mission Management

Signals Intelligence mission management consists of the unit commander's supervision of collection, processing (including language translations), production, and dissemination efforts. Proper mission management requires centralized control of SIGINT assets at the MAGTF CE level and ensures assets work on collection or analysis efforts addressed by other SIGINT elements. Mission management also ensures SIGINT authorities approve missions, and those missions remain valid.

Collection and geolocation elements are usually positioned throughout the MAGTF's AO based on the MAGTF's focus of effort, scheme of maneuver, discovery of enemy signals, and security of SIGINT units. SIGINT operations supporting both ACE and MAGTF requirements will be planned and incorporated in the supporting air tasking order.

Signals Intelligence unit commanders and planners must ensure that coverage is complete, assets are gainfully employed or redirected, and SIGINT reporting is effective. They must also analyze collection tasks to determine if the tasks are still valid or if new collection or analysis efforts are required. The collection, DF, and analysis and production efforts must be supervised, integrated with all source intelligence operations, and evaluated to ensure mission effectiveness.

Signals Intelligence Collection, Processing, and Execution Planning

During collection, SIGINT elements collect and deliver information to the appropriate processing or production element. In the MAGTF, the goal is to exploit organic collection with organic resources. In some cases, the MAGTF may exploit the collection from national or theater collection assets. In other cases, the MAGTF may require support from theater or national processing or production nodes. The MAGTF SIEW teams, OCEs, and the OCAC will deliver SIGINT derived threat warning information directly to affected commanders for immediate action. Signals Intelligence collection is closely tied to the processing and exploitation phase, as explained previously in this chapter.

Signals Intelligence collection and processing and exploitation planning should consider the appropriate type and placement of equipment. Due to the limited space available in mobile platforms, OCEs must prioritize the most relevant signals and create the collection, processing, and exploitation package for each team, as directed by the OCAC. Fixed site operations are limited only by the security provided and access to the signals. Dense signal environments will increase the number of separate systems.

The flight path is critical to SIGINT operations for air platforms, as is the architecture to move data. The SIEW teams supporting the ACE will often be SCI radio relay teams positioned to move the data back to OCEs or the OCAC. In other cases, the ACE SIEW team may control EW capabilities or the SIGINT payloads. In the latter scenario, teams supporting ACE SIGINT platforms will need capabilities to process and exploit the data and move the raw SIGINT reports back to an OCE or the OCAC.

The availability of cryptologic language analysts to exploit collected signals is a critical collection planning consideration. The MAGTF rarely has enough linguists, whether positioned forward with collection teams or massed at OCEs or the OCAC. Therefore, the MAGTF must effectively use Marine cryptologic language analysts, other service linguists, and contract linguists.

Signals Intelligence Collection Planning Considerations

There are several considerations for SIGINT collection planning that are dependent on physical terrain to ensure access to the target signal(s).

Topography. Terrain, physical obstructions, and vegetation in the AO have a major effect on the employment of SIGINT resources and the ability to exploit enemy signals. Proper placement of SIGINT collection and geolocation assets is essential for effective reception and exploitation of adversary emanations. Geolocation operations are especially dependent on terrain. Due to a phenomenon known as multi-pathing, a frequency will bounce off structures and may appear to come from several locations. This may require more than one SIGINT asset to locate a target, or for a ground based SIGINT team to be mobile.

Several factors other than topography and environment affect reception quality. For most collection operations, signal quality is the most important factor affecting collection, determined by the frequency, power of the transmitter, and the antenna and amplifier used for collection.

Target Frequencies. Many of the frequency ranges and power levels in use by the world's military and paramilitary forces require line of sight (LOS) or near LOS paths from transmitter to receiver. Generally, the higher the frequency used, the greater the requirement for LOS. Therefore, the accurate placement of SIGINT collection and geolocation equipment is more critical for higher frequencies.

Lower frequencies (particularly those below 30 MHz) generally do not require LOS paths. Consequently, the MAGTF may locate these SIGINT collection and geolocation sites at greater distances from the target transmitters to exploit these frequencies. These frequencies can possibly be collected from outside the AO.

Power Output. The power output of a transmitter is an important factor in receiving the signal. The MAGTF must locate SIGINT collection and geolocation assets closer to the adversary's transmitter to intercept some low-powered signals. This often requires SIGINT collection and geolocation teams to either collocate with or closely follow forward MAGTF combat units.

Antennas. The distance at which Marine SIGINT teams must position themselves from the target is determined by the type of antenna used by the target to transmit and the antenna type SIGINT uses to intercept the signal. If the targeted adversary's system uses highly directional antennas, as do many multichannel systems, teams must locate their SIGINT collection and geolocation site(s) within the adversary's antenna radiating pattern. Due to increased signal strength, however, they may increase their distance from the target.

Signals Intelligence Collection. Signals Intelligence collection may require close access to a collection target, or it may allow for collection from locations far removed from the AO. The targeted signal may require specialized equipment, purpose built for the signal, or it may require national level assistance with decrypting and decoding. In other cases, locally available commercial off-the-shelf equipment may be adequate for the signal environment. Depending on the mode of communications, the linguists may need to be as proficient in reading the target language as they are in listening.

Signals Intelligence planners must understand the unique considerations of COMINT collection. Tactical Marine SIGINT can provide collection against many, but not all, signals that will be found in the battlespace. Planners should identify the physical and technological SIGINT gaps organic assets can satisfy and then work with the collection manager to request theater and national SIGINT capabilities to fill any remaining gaps. In many cases, the coordination for national SIGINT capabilities will be between the MAGTF OCAC and the NCR in theater and the Marine Cryptologic Office at NSA.

Due to organic collection limitations, the MAGTF may require theater or national assistance to collect, process and exploit SIGINT. If possible, planners should try to fill the technological gap with a request for non organic equipment, and staff the equipment with organic personnel. If the gap is only limited in duration or covers too much geographic area for organic equipment and personnel, SIGINT planners should request theater airborne SIGINT support (aka medium altitude SIGINT) via the IOC or theater collection managers.

Locating signals through collection requires appropriate assets, coordination, and planning. The SIGINT planner must ensure that geolocation personnel have appropriate gear and training, and that operational checks are performed prior to mission execution.

Direction finding requires at least three outstations and, ideally, planners should ensure every SIGINT element is always DF and/or PGL capable. This will alleviate some of the requirements to move assets around the battlespace. It is easier to use an asset already in place or close by than to move several assets from one side of the AO to another. Technology has enabled greater tipping and cueing between multiple theater and national DF assets to the extent that at least three outstations are now required to achieve a baseline. The Marine Corps is moving towards interoperability with any theater or national DF asset.

Under many circumstances, organic DF assets may be all that are available. Planners need to ensure that organic DF assets are employed to create usable results. If the mission is to DF a specific target or signal environment, the MAGTF can accomplish this by placing the teams in a non linear network with moderate separation from each other. The target and terrain determine moderate separation. The assets will need to be close enough to each other to have good audio on the target and, if possible, teams should place DF assets with unrestricted LOS (e.g., teams should not place assets on the opposite side of a mountain from the target). The assets will need enough separation to get distinct measurements from site to site. If the assets are too close together or parallel, the location may be incalculable or the error rate so high that the location is irrelevant.

Signals Intelligence, G-2/S-2, and G-3/S-3 planners should remain flexible and move DF assets to better locations when results are inconclusive. Although it is not ideal, if assets are limited, a single LOB can be useful.

A realistic employment scenario is to attach DF assets with maneuver elements. While this often does not present optimal opportunities to fix targets, organic DF operations can be useful for I&W. Coupled with SIGINT processing, exploitation, and terrain and order of battle analysis, DF operations can provide locations to tip and cue other ISR assets or provide vectors towards enemy formations.

Processing and Exploitation

The following processing and exploitation functions are used to convert collected raw information into a form suitable for SIGINT production.

Traffic Analysis. Traffic analysis is the study of all COMINT characteristics of communications, except encrypted texts. Call signs, frequencies, times of transmission, cryptographic indicators, precedence, and message lengths are examples of these characteristics.

Cryptanalysis. Cryptanalysis is the study of encrypted signals, data, and texts to determine their plain language equivalents. The capability to read the adversary’s encrypted communications is obviously valuable.

The Marine Corps has no cryptanalysis capability. The National Security Agency accomplishes this function.

Linguistic Analysis. Linguistic analysis is the transcription and translation of foreign language intercepts into English. This analysis starts at the collection site upon interception. Messages of considerable length require more time and are usually transcribed and translated at the OCE, OCAC, or other production nodes within the USSS. Marines train in a wide variety of languages for this task, but augmentation by external sources (e.g., native and/or contract linguists) may be required to satisfy all requirements.

Signal Analysis. Signal analysis consists of working with all types of signals (e.g., COMINT, ELINT, Proforma) to identify, isolate, reduce to pure form, and exploit acquired SOIs. The signal analyst must be well trained and possess the proper electronic and software support tools to be effective.

Electronic Intelligence Analysis. The location of radar can provide a general trace of the adversary's forward battle positions and locations of key C2 and fire control nodes and weapons systems. Medium range and counter weapons radar identification provides order of battle information since these systems are organic to specific adversary units.

Identifying and locating air defense radar provides information on the disposition of the adversary's air defense systems and their threat to friendly strike aircraft, close air support, and assault support aircraft.

Following the reporting of any I&W information to tactical decision makers, SIEW teams forward technical data and detailed ELINT information to the OCAC EW/S-3 section for further analysis, production, and reporting.

SIGNALS INTELLIGENCE ANALYSIS AND PRODUCTION

Production converts raw information into SIGINT product reports through the evaluation, integration, and interpretation of the information derived during the processing and exploitation effort.

In some cases, the collection (to include geolocation), basic processing, and basic exploitation of certain signals in the EMS is not SIGINT but is categorized as ES. If the collected information remains unevaluated and used for immediate threat recognition, targeting, planning, and future operations, it is not SIGINT. In other cases, specialized equipment and processes make the collection of signals SIGINT from the outset. In all cases though, retaining processed signals to evaluate the relevance and utility of a signal's technical information and content is SIGINT (COMINT or ELINT).

The process to evaluate a signal's technical aspects and content is SIGINT analysis. The SIGINT analysts correlate multiple signal intercepts and, working with SIGINT reporters, produce SIGINT reports.

These raw SIGINT reports are provided directly to tactical commanders for threat warning via the most expeditious means. In some cases, direct reporting to MSC intelligence, operations, and targeting sections is required and will be documented in the RadBn RP&G. The Marine Cryptologic Office maintains the NSA approved RP&G.

The OCAC receives all raw SIGINT reports from within the MAGTF AO and provides tactical and evaluated SIGINT reports to the G-2/S-2s to further analyze and produce all source intelligence. The OCAC also provides evaluated reports to the staff sections for future operations planning.

Signals Intelligence production planning and management are closely coordinated with all source intelligence production planning and management to—

- Determine the scope, content, and format for each product.
- Develop a plan and schedule for the development of products.
- Assign priorities among the various SIGINT product requirements.
- Allocate SIGINT processing, exploitation, and production resources.
- Integrate production efforts with all-source collection and dissemination activities.

SIGNALS INTELLIGENCE DISSEMINATION AND INTEGRATION

Dissemination is providing SIGINT information in a timely manner and in a usable form to commanders, other decision makers, and all-source intelligence analysts. Because of security requirements, dissemination of COMINT information is made primarily to SIGINT and all source intelligence production elements such as the MAGTF IOC. Proper SIGINT C2 and supporting ISR data architectures enable proper dissemination. Effective IRs and tactical requirements management, to include providing combat information for force protection, targeting, and situational awareness, are part of any dissemination plan.

Signals Intelligence dissemination planning and management involves establishing dissemination priorities, stipulating dissemination and reporting criteria, selecting dissemination means, and monitoring the flow of SIGINT reporting. The ultimate dissemination goal is to deliver SIGINT products to the appropriate user in the proper form and at the right time while concurrently preventing disseminating irrelevant products and avoiding information overload.

Reporting consists of providing SIGINT in standardized formats. The nature of the SIGINT effort requires timely reporting to effectively exploit its intelligence value. The SIGINT reports generally fall into two categories: tactical SIGINT reports and technical reports. Standardized formats are used when preparing and transmitting these reports for speed and compatibility. As most of these formats are classified, readers should refer to SIGINT reporting directives for specific formats and examples.

Reports

Tactical SIGINT Reports. Tactical SIGINT producers and consumers prepare tactical SIGINT reports for commanders, planners, and all source intelligence analysts. A tactical SIGINT report contains timely, accurate, thorough, relevant, and useful information derived from SIGINT processes about the adversary in response to the supported commander's PIRs and IRs. In accordance with specified intelligence reporting criteria, reports may be sent periodically or whenever highly perishable data is acquired. Tactical SIGINT reporting follows the formats, rules, and regulations set forth in Time-Sensitive SIGINT Reporting Directives.

In tactical SIGINT reports, the source of information is clearly identified as SIGINT by the content and classification markings. Such reports generally contain the SIGINT assessment along with pertinent SIGINT technical information. Analysts process these reports within the SCIF/SCI communications channels to develop releasable SIGINT to designated recipients on the appropriate network/classification. Within a MAGTF, the CE, GCE, and ACE may be recipients on distribution lists for SIGINT products. All recipients should recognize SIGINT reports as sole source. To clearly understand the battlespace usually requires fusion with other intelligence sources. When pertinent, dissemination can be conducted via SCI courier or compartmented briefings.

A special kind of SIGINT report is the non code word (NCW) report. Procedures for an NCW report are used only when authorized by DIRNSA. The principal value of NCW reporting is to allow time sensitive dissemination of critical SIGINT information to a broader audience during high tempo combat operations. In NCW reports, the source of information is clearly SIGINT. However, unlike standard SIGINT product reports, the NCW report is passed directly to commanders without SIGINT markings or SCI security controls to allow immediate tactical use (e.g., I&W, support to targeting, support to force protection). For example, NCW reports may be passed directly from the SIEW team to other MAGTF units (e.g., an infantry battalion) via GENSER communications (usually voice message). Typically, the format for these is the standard SALUTE (size, activity, location, unit, time, and equipment) report. Non-codeword reporting follows the formats, rules, and regulations set forth in NCW reporting program directives. Any time a MAGTF is involved in combat operations, NCW reporting is an implied task. The Marine Cryptologic Office coordinates with the DIRNSA/CHCSS prior to the start of operations to gain NCW reporting authority.

Specific procedures regarding NCW reporting during operations should be contained within the SIGINT appendix to Annex B of the OPORD and captured in the RP&G.

Sanitized Reports. Sanitized SIGINT reports contain information reported via GENSER communications in a manner that does not reveal SIGINT as the source of the information. DODD TS 5105.21 M 2, *SCI Security Manual, Communications Intelligence Policy* establishes the MAGTF commander's level of sanitization authority.

Within the MAGTF, designated intelligence personnel under the guidance and supervision of the MAGTF SSO, IOC OIC, and the dissemination officer generally perform the actual sanitization of SIGINT reports. Marine SIGINT analysts are trained as reporters and receive sanitization training. During exercises, sanitization should be a measured event. The sanitized reports are further disseminated as all source products or other GENSER intelligence reports.

Technical Reports. Technical reports consist of the SIGINT technical elements required by SIGINT collectors, analysts, and technical support and production agencies external to the MAGTF (e.g., call signs, frequencies, operating schedules). Signals Intelligence technical reporting requires SCI secure connectivity with pertinent organizations (e.g., NSA, theater SIGINT elements, and members of the Marine Corps SIGINT community) via JWICS, NSANET, or some alternate SCI communications means. Within the MAGTF, either the RadBn or the ACE's EW section conducts all SIGINT technical reporting.

Signals Intelligence Integration Products

Analysts must fully integrate the information derived from traffic analysis, cryptanalysis, linguistic analysis, signal analysis, ELINT analysis, and radio geolocation into a fused SIGINT product to develop a complete SIGINT picture. Concurrently, integration of SIGINT processing and production with ongoing MAGTF G-2/S-2 all source intelligence processing and production is essential to achieve a complete, effective, and current intelligence estimate while using the strengths and results from other intelligence disciplines to improve SIGINT operations.

Signals Intelligence has no inherent value to MAGTF operations. Its value is realized only through its effective support of the commander's IRs or other operational requirements. Commanders, G-2/S-2s, and G-3/S-3s must continuously evaluate SIGINT operations, products, and reports for timeliness, usefulness, and overall quality and responsiveness to stated IRs. They must provide feedback to the MAGTF G-2/S-2 and SIGINT unit leaders to improve future SIGINT operations. Ultimately, SIGINT utilization guides future intelligence and SIGINT operations and management.

SIGNALS INTELLIGENCE EVALUATION AND FEEDBACK

Signals Intelligence analysts evaluate the raw SIGINT information to determine its pertinence to IRs. The SIGINT senior analysts and all source analysts further evaluate the information to isolate significant elements and determine the information's reliability and accuracy. Commanders, planners, and other staff provide feedback to ensure that SIGINT is meeting their information needs. From that feedback, the RadBn OCAC directs SIGINT operations against specific signals and renews the process for follow on requirements that may come up.

SIGNALS INTELLIGENCE ORDERS DEVELOPMENT

The MAGTF G-2/S-2 is responsible for tasking the MAGTF's SIGINT assets. The MAGTF G-3/S-3 is responsible for tasking the MAGTF's EW and cyberspace operations assets. The base order and fragmentary orders are the mechanisms to employ SIGINT assets in the battlespace. The base order defines the concept of intelligence, fires, and cyberspace operations in annexes and appendices. The executing elements conduct their mission analysis based on these higher orders, along with the constraints and restraints identified in national and theater SIGINT, EW, and cyber orders and policies, and develop their orders to their subordinate assets. Although the G-2/S-2 maintains staff cognizance over the RadBn or the detachment, the RadBn commander and staff must consider the EW and cyber tasks and provide feedback to the G-2/S-2 and G-3/S-3 when the direction and tasking are inconsistent or require deconfliction.

The SIGINT appendix will appear as Appendix 2 (signals intelligence) to Annex B (intelligence) in all MAGTF operations plans and orders. (See Annex A, titled "Annex B of an Operation Order," of this publication for a recommended format for the SIGINT appendix.) It should include the following:

- Friendly forces to be utilized include:
  - Personnel augmentation requirements.
  - SIGINT units of adjacent or other theater forces and the support expected.
  - Joint force maritime component commander, DS SIGINT elements, and Combatant Service Support Area available to support the landing force during amphibious operations.
  - RSOC, joint force land component commander, joint force air component commander, and other component commanders or task forces capable of providing SIGINT support during JTF operations.
- Planned arrangement, employment, and use of external SIGINT support, to include any special collection, production, dissemination, and CIS arrangements.
- Coordinating instructions for SIGINT operations planning and control, to include technical support expected from higher headquarters.
- Tasking to MAGTF SIGINT elements (deconflicted and prioritized with EW and cyber tasking).
- SIGINT communications architecture and information management.

SIGNALS INTELLIGENCE EXECUTION

The MAGTF's SIGINT operations generally are centrally managed by the MAGTF G-2/S-2 and decentrally executed to—

- Integrate MAGTF SIGINT effectively with other MAGTF and external intelligence and reconnaissance operations.
- Provide the most effective MAGTF IR support.

Integrating SIGINT collection, production, and dissemination plans and activities with those of other MAGTF and supporting intelligence organizations provides more efficient and effective use of limited resources and increases the mutual support intelligence assets can provide across geographic boundaries (e.g., cueing). The MAGTF mission, commander's intent, threat operations and signals usage, concept of operations, and environmental considerations all influence the ultimate task organization, command relationship, concepts of employment, and tasks of SIGINT units.

Such information is specified within annexes B, C, and K of the OPORD or subsequent fragmentary order. The following are key aspects of these interrelated SIGINT operations:

- Task organization and command or support relationships of MAGTF SIGINT units with other MAGTF elements. The OPORD must explicitly task the critical support relationships to ACE, GCE, and LCE commanders. The SIEW teams and OCEs require support over and above typical GS and DS relationships, to include security, logistics, and maintenance. The return on investment for the local commanders is I&W, targeting, and SCI communications support while the SIGNT element is collocated.
- External SIGINT units that typically support a MAGTF.
- Principal SIGINT systems employed within, and in support of, the MAGTF.
- Relationship of other MAGTF intelligence and reconnaissance units with SIGINT units.
- Principal communications pathways, means, and level of classification.
- Key intelligence information systems that interoperate with SIGINT systems.
- Principal SIGINT reports disseminated via the communications pathways shown.

APPENDIX A. RADIO BATTALION SIGINT/EW SUPPORT DETACHMENT CHECKLISTS

The following checklist is provided as a guide to assist the RadBn SIGINT/EW (SIEW) support detachment OIC conduct operations. Depending on the mission, location, and duration of an operation, some items may not be applicable.

PLANNING STAGE

❑ Coordinate with the RadBn S-3 to:

___ Determine exact mission and tasking of the detachment and the authority and command relationship.

___ Review all messages related to deployment and composition of the detachment.

___ Ensure S-3 tasks companies or sections to provide required personnel to fill detachment T/O line numbers.

___ Request assignment of RadBn SIGINT address and producer designator digraph, if necessary.

___ Verify formats and instructions for required reports.

___ Determine if area clearances and clearance certifications are necessary and request SSO take appropriate action.

___ Review pertinent orders and instructions of the supported unit.

___ Identify and arrange for special training and operational requirements.

❑ Coordinate with the following supported command:

___ G-2/S-2 IOO to determine initial intelligence collection, production, and dissemination requirements and current intelligence estimate.

___ G-2/S-2 IOO to determine time constraints for submission of input to appendix 2 to annex B of the OPORD.

___ G-2/S-2 all source fusion center OIC to determine plans and integration of intelligence and SIGINT production activities.

___ G-2/S-2 dissemination officer for a list of SIGINT products recipients, appropriate report formats, and routine and time sensitive CIS plans.

___ G-2/S-2 IOO and G-4/S-4 for supply and logistics requirements to be provided by supported command (e.g., electronic maintenance and consumables such as batteries; meals, ready to eat; maps; and fuel).

___ G-3/S-3 electromagnetic warfare officer for EA requirements and capabilities and input to appendix 3 to annex C of the OPORD.

___ G-2/S-2 operations officer and G-6/S-6 to address requirements for communications support (e.g., secure and unclassified LAN access, equipment).

___ G-3/S-3 to establish liaison teams with supported unit's subordinate elements if necessary.

___ Command security manager, G-2/S-2, and G-3/S-3 for force protection and communications security monitoring requirements and plans.

❑ Develop and publish a training schedule in coordination with the RadBn S-3 and supported unit's intelligence officer.

❑ Request courier cards from RadBn SSO for appropriate detachment personnel.

❑ Coordinate collection and analytical and production requirements with the OCA element to:

___ Ensure the detachment analytical and production team knows the technical aspects of the operations area.

___ Ensure the analytical and production team has a current technical support package; request an update if required (i.e., hardcopy, electronic copy).

___ Ensure SIGINT position designators for equipment are current; prepare and issue required SIGINT Resource Status Report.

___ Ensure the NSA or the pertinent regional security operations center or cryptologic shore support activity provides a current technical briefing on targets in the AO.

❑ Coordinate transportation requirements with RadBn S-3, S-4, and supported unit.

❑ Coordinate embarkation requirements with RadBn S-4 and supported unit to:

___ Review current embarkation orders.

___ Complete embarkation forms (e.g., Tactical Cargo Manifest Declaration, 1387-2, 1348-1).

___ Review current inbound and outbound agricultural restrictions on vehicles.

___ Assemble complete embarkation kit with guidelines for use upon departure.

___ Request T/E items for detachment.

❑ Coordinate communications and information requirements with RadBn S-6 and supported unit intelligence officer and CIS officer to:

___ Determine circuit request requirement.

___ Determine Telecommunications Service Request requirement.

___ Determine frequency and call sign requirements and request communications electronics operating instructions.

___ Request Special Intelligence (SI) routing indicator and plain language address assignments.

___ Determine Communications Security Materials System (CMS) requirements and request that the CMS custodian have material available for issue.

___ Designate an SSO CMS custodian.

___ Determine TEMPEST inspections and automated information systems accreditation requirements.

___ Determine cryptographic hardware and keying material requirements and procedures with all communication elements.

❑ Ensure all personnel are qualified with T/O weapons and arrange for Battlesight Zero (BZO), firing as necessary.

PREDEPLOYMENT STAGE

❑ Audit health records to:

___ Determine inoculations required and arrange for required shots with the corpsman.

___ Determine if detachment members or members of their families are undergoing extensive outpatient care, with an indefinite prognosis.

___ Confirm and record blood types.

___ Ensure all personnel requiring eyeglasses have two pair. Also ensure they have optical inserts for gas masks.

___ Ensure detachment members meet class I or II dental readiness.

___ Arrange for block pickup of health and dental records.

❑ Coordinate legal affairs to:

___ Inform personnel of advisability of wills and procedures for obtaining them.

___ Inform personnel of powers of attorney and procedures for obtaining them.

❑ Arrange for storage of privately owned vehicles and personal effects.

❑ Arrange for mail handling.

❑ Coordinate pay matters to:

___ Conduct personal financial record audit.

___ Prepare savings and other allotments.

❑ Coordinate administrative matters to:

___ Verify accuracy of record of emergency data.

___ Ensure identification cards are current and have proper Geneva Convention category information.

___ Ensure personnel have current Identification (ID) tags.

___ Audit and update officer qualification records and enlisted service record books.

___ Complete change of reporting senior fitness reports, fitness report roughs, and proficiency and conduct marks.

❑ Coordinate clothing inspection and requirements to:

___ Ensure personnel have appropriate serviceable uniforms for all destinations.

___ Ensure personnel have appropriate civilian attire in accordance with local military customs of country(ies) to be visited.

___ Ensure temporary issue requirements draw includes the proper sizes and is coordinated through the RadBn S-4 and supported unit.

❑ Ensure baggage is appropriate and of sturdy construction.

❑ Ensure personnel know customs requirements of locations to be visited.

❑ Prepare government transportation request.

❑ Prepare military transportation authorization.

❑ Conduct the following:

___ Family services deployment briefing for all SIEW support detachment Marines and family members.

___ Red Cross brief.

___ Navy and Marine Corps Relief brief (to include preauthorized emergency loan applications).

___ Religious services brief.

___ Family services brief.

___ Key spouses brief.

❑ Assemble assigned T/E equipment required for deployment to:

___ Perform operational check of equipment.

___ Complete Limited Technical Inspection (LTI) on all equipment.

___ Perform acceptance inspections on all temp loan equipment.

___ Check the date of last calibration, if applicable.

❑ Arrange for draw or transfer of CMS material.

❑ Receive CMS custodial briefing from CMS custodian.

❑ Receive security requirements and emergency destruction briefing from SSO.

❑ Conduct training in accordance with established detachment training schedule.

❑ Coordinate with the RadBn SSO and classified materials control officer to:

___ Designate a detachment classified material secondary control point and custodian.

___ Ensure required single-scope background investigation periodic reviews are initiated on those detachment personnel identified as needing updates.

___ Request SCI clearance certification on all detachment personnel be forwarded to cognizant units and other organizations, as necessary.

❑ Coordinate with the RadBn adjutant or S-1 to:

___ Draw record books.

___ Pick up orders.

___ Establish report criteria.

___ Arrange for administrative and legal briefs.

___ Arrange for detachment Uniform Code of Military Justice and code of conduct briefings.

❑ Coordinate with RadBn SSO to:

___ Confirm security requirements.

___ Pick up courier cards for specified personnel.

___ Receive area intelligence briefs to include customs, politics, religion, and standards of personal conduct.

___ Receive counterintelligence area threat briefs.

___ Ensure all required personnel receive appropriate special access indoctrination(s).

___ Transfer necessary technical material from SSO and OCA classified material control center accounts.

❑ Coordinate with RadBn S-3 to:

___ Establish SIGINT operations report criteria.

___ Determine topographic and map requirements and request allowance from OCA or the supported unit.

___ Request preparation of appropriate cryptologic technical kits from NSA or the supporting cryptologic shore support activity.

❑ Coordinate with RadBn S-4 supply to establish fiscal account job order numbers and sign the consolidated memorandum receipt.

❑ Coordinate with RadBn S-4 electronic maintenance to:

___ Establish equipment maintenance procedures.

___ Establish electronic maintenance support and prepare pre-expend bin support block.

___ Ensure that all equipment receives a predeployment LTI.

___ Ensure skeleton record jackets are prepared for all equipment.

❑ Coordinate with RadBn S-4 motor transport and engineer to:

___ Establish equipment maintenance procedures.

___ Establish motor transport and engineer support.

___ Ensure skeleton record jackets are prepared for all vehicles.

❑ Coordinate with RadBn S-4 ordnance officer to:

___ Determine weapon requirements and other ordnance needs.

___ Obtain proper storage boxes for the transport of weapons.

___ Draw weapons.

___ Conduct necessary inspections.

___ Conduct daily sight counts.

___ Determine ammunition and pyrotechnic training requirements during deployment.

❑ Coordinate with RadBn S-4 embarkation officer to:

___ Receive embarkation package.

___ Determine dunnage requirements.

❑ Draw equipment and sign for gear assigned to detachment.

❑ Receive medical brief from battalion medical personnel.

❑ Contact special services officer for recreation items.

❑ Publish the final:

___ Detachment T/O and T/E.
___ Roster of personnel.
___ Dependent point-of-contact roster.
___ Equipment and uniforms required.
___ Detachment training schedule.
___ Detachment OPORD.

❑ Palletize or combat load supplies and equipment.

❑ Coordinate embarkation of personnel and equipment with S-4 of supported unit.

___ Stage for embarkation.

DEPLOYMENT

❑ Coordinate with G-2/3 and S-2/3 for initial location of combat operations center, combat intelligence center, and collection DF and EA teams.

❑ Continue coordination of collection and DF team and RRT locations with G-2/S-2 collections officer and G-3/S-3. Include updates for inserts, extract times, and methods.

❑ Coordinate with G-2/S-2 IOO for inputs and presentation for intelligence estimate, concept of operations, and intelligence operations plans briefings.

❑ Submit the following required reports and messages:

___ Activation report and deactivation report to RadBn S-3 and supported unit G-2/S-2.
___ Circuit activation report to RadBn S-6 and supported unit G-6/S-6.
___ Administrative reports to RadBn S-1.
___ CMS destruction reports to SSO or CMS.
___ Circuit deactivation report to RadBn S-6 and supported unit G-6/S-6.
___ Transportation request to RadBn and supported unit G-4/S-4.
___ Required analysis and technical reports to OCA and supported unit G-2/S-2. (Resource Status Report NSA upon activation and deactivation.)
___ Tactical SCI facility activation and deactivation reports to Commander, Naval Security Group, supported unit SSO, and others as appropriate.

❑ Prepare and distribute required reports to the supported commander.

❑ Send deactivation message.

POSTDEPLOYMENT

- ❑ Turn in weapons and classified material immediately upon return.
- ❑ Participate in supported unit operations debriefings as required. Debrief with RadBn CO and S-3 on the first working day after return.
- ❑ Coordinate with RadBn adjutant, S-1, S-3, and S-4 to:

  ___ Return record books to S-1.

  ___ Return medical and dental records.

  ___ Terminate temporary additional duty orders.

  ___ Prepare and submit performance evaluation reports and proficiency and conduct marks as required for the temporary additional duty period.

  ___ Notify mail clerk to stop forwarding mail.

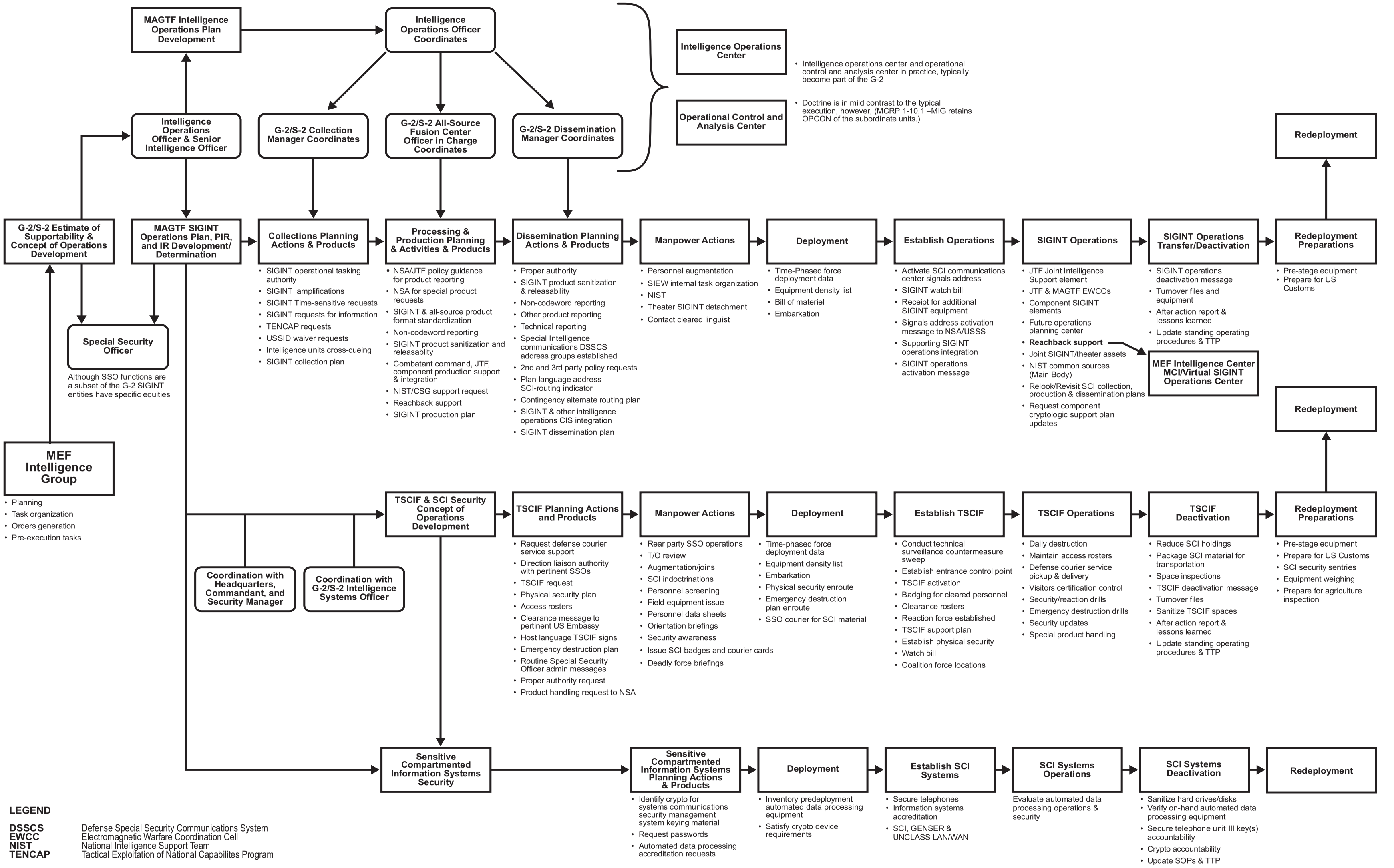
  ___ Return technical material to the OCA platoon.
- ❑ Return CMS material to CMS custodian within 48 hours of return.
- ❑ Return courier cards to SSO.
- ❑ Prepare equipment for postdeployment LTI.
- ❑ Ensure proper maintenance is conducted on equipment prior to returning to respective companies or sections.
- ❑ Turn in equipment-on-equipment repair orders and note any equipment damage or problems.
- ❑ Settle fiscal account.
- ❑ Submit an after-action report within 20 days of return (or as directed) to the supported unit G-2/S-2, G-3/S-3, and RadBn S-3.
- ❑ Disband detachment.
- ❑ Prepare award recommendations on deserving personnel.
- ❑ Recommend necessary changes to unit SOPs and coordinate with the RadBn and supported unit staff.

(U) APPENDIX B. MARINE CORPS SIGINT/EW PROGRAMS OF RECORD AND THE REQUIREMENTS PROCESS

Appendix B contains controlled unclassified information and has been removed. A full copy of the publication can be obtained at https://usmc.sharepoint-mil.us/sites/MCEN_Support_MCDoctrine.

APPENDIX C. SIGINT AND SCI SECURITY MANAGEMENT OPERATIONS FLOWCHART

The flowchart on the following pages summarizes the principal SIGINT and SCI security planning considerations, activities, and products discussed in this publication.


MAGTF Intelligence Operations Plan Development
Intelligence Operations Officer Coordinates
Intelligence Operations Center
Operational Control and Analysis Center
• Intelligence operations center and operational control and analysis center in practice, typically become part of the G-2
• Doctrine is in mild contrast to the typical execution, however, (MCRP 1-10.1 –MIG retains OPCON of the subordinate units.)
Intelligence Operations Officer & Senior Intelligence Officer
G-2/S-2 Collection Manager Coordinates
G-2/S-2 All-Source Fusion Center Officer in Charge Coordinates
G-2/S-2 Dissemination Manager Coordinates
G-2/S-2 Estimate of Supportability & Concept of Operations Development
MAGTF SIGINT Operations Plan, PIR, and IR Development/ Determination
Collections Planning Actions & Products
• SIGINT operational tasking authority
• SIGINT amplifications
• SIGINT Time-sensitive requests
• SIGINT requests for information
• TENCAP requests
• USSID waiver requests
• Intelligence units cross-cueing
• SIGINT collection plan
Processing & Production Planning & Activities & Products
• NSA/JTF policy guidance for product reporting
• NSA for special product requests
• SIGINT & all-source product format standardization
• Non-codeword reporting
• SIGINT product sanitization and releasablity
• Combatant command, JTF, component production support & integration
• NIST/CSG support request
• Reachback support
• SIGINT production plan
Dissemination Planning Actions & Products
• Proper authority
• SIGINT product sanitization & releasability
• Non-codeword reporting
• Other product reporting
• Technical reporting
• Special Intelligence communications DSSCS address groups established
• 2nd and 3rd party policy requests
• Plan language address SCI-routing indicator
• Contingency alternate routing plan
• SIGINT & other intelligence operations CIS integration
• SIGINT dissemination plan
Manpower Actions
• Personnel augmentation
• SIEW internal task organization
• NIST
• Theater SIGINT detachment
• Contact cleared linguist
Deployment
• Time-Phased force deployment data
• Equipment density list
• Bill of materiel
• Embarkation
Establish Operations
• Activate SCI communications center signals address
• SIGINT watch bill
• Receipt for additional SIGINT equipment
• Signals address activation message to NSA/USSS
• Supporting SIGINT operations integration
• SIGINT operations activation message
SIGINT Operations
• JTF Joint Intelligence Support element
• JTF & MAGTF EWCCs
• Component SIGINT elements
• Future operations planning center
• Reachback support
• Joint SIGINT/theater assets
• NIST common sources (Main Body)
• Relook/Revisit SCI collection, production & dissemination plans
• Request component cryptologic support plan updates
MEF Intelligence Center MCI/Virtual SIGINT Operations Center
SIGINT Operations Transfer/Deactivation
• SIGINT operations deactivation message
• Turnover files and equipment
• After action report & lessons learned
• Update standing operating procedures & TTP
Redeployment Preparations
• Pre-stage equipment
• Prepare for US Customs
Redeployment
Special Security Officer
Although SSO functions are a subset of the G-2 SIGINT entities have specific equities
MEF Intelligence Group
• Planning
• Task organization
• Orders generation
• Pre-execution tasks
TSCIF & SCI Security Concept of Operations Development
Coordination with Headquarters, Commandant, and Security Manager
Coordination with G-2/S-2 Intelligence Systems Officer
TSCIF Planning Actions and Products
• Request defense courier service support
• Direction liaison authority with pertinent SSOs
• TSCIF request
• Physical security plan
• Access rosters
• Clearance message to pertinent US Embassy
• Host language TSCIF signs
• Emergency destruction plan
• Routine Special Security Officer admin messages
• Proper authority request
• Product handling request to NSA
Manpower Actions
• Rear party SSO operations
• T/O review
• Augmentation/joins
• SCI indoctrinations
• Personnel screening
• Field equipment issue
• Personnel data sheets
• Orientation briefings
• Security awareness
• Issue SCI badges and courier cards
• Deadly force briefings
Deployment
• Time-phased force deployment data
• Equipment density list
• Embarkation
• Physical security enroute
• Emergency destruction plan enroute
• SSO courier for SCI material
Establish TSCIF
• Conduct technical surveillance countermeasure sweep
• Establish entrance control point
• TSCIF activation
• Badging for cleared personnel
• Clearance rosters
• Reaction force established
• TSCIF support plan
• Establish physical security
• Watch bill
• Coalition force locations
TSCIF Operations
• Daily destruction
• Maintain access rosters
• Defense courier service pickup & delivery
• Visitors certification control
• Security/reaction drills
• Emergency destruction drills
• Security updates
• Special product handling
TSCIF Deactivation
• Reduce SCI holdings
• Package SCI material for transportation
• Space inspections
• TSCIF deactivation message
• Turnover files
• Sanitize TSCIF spaces
• After action report & lessons learned
• Update standing operating procedures & TTP
Redeployment Preparations
• Pre-stage equipment
• Prepare for US Customs
• SCI security sentries
• Equipment weighing
• Prepare for agriculture inspection
Redeployment
Sensitive Compartmented Information Systems Security
Sensitive Compartmented Information Systems Planning Actions & Products
• Identify crypto for systems communications security management system keying material
• Request passwords
• Automated data processing accreditation requests
Deployment
• Inventory predeployment automated data processing equipment
• Satisfy crypto device requirements
Establish SCI Systems
• Secure telephones
• Information systems accreditation
• SCI, GENSER & UNCLASS LAN/WAN
SCI Systems Operations
Evaluate automated data processing operations & security
SCI Systems Deactivation
• Sanitize hard drives/disks
• Verify on-hand automated data processing equipment
• Secure telephone unit III key(s) accountability
• Crypto accountability
• Update SOPs & TTP
Redeployment
LEGEND
DSSCS Defense Special Security Communications System
EWCC Electromagnetic Warfare Coordination Cell
NIST National Intelligence Support Team
TENCAP Tactical Exploitation of National Capabilites Program

APPENDIX D. SIGNALS INTELLIGENCE APPENDIX FORMAT

An operations order (OPORD) contains 21 annexes, many of which include appendices. Annex B is used for intelligence and provides detailed information about the adversary and battlespace. This annex also provides guidance on intelligence and counterintelligence functions. Appendix 2 of Annex B contains SIGINT-specific information. It includes two tabs—Tab A: Communications Intelligence Collection Requirements, and Tab B: Operational Electronic Intelligence Collection Requirements.

Appendix 2 should explain how SIGINT elements, either supporting or OPCON to the MAGTF, will be used to support the OPORD. The appendix should also provide guidance to subordinate commanders for conducting SIGINT operations and supporting SIGINT elements and personnel identified to fulfill SIGINT requirements identified in the OPORD.

CLASSIFICATION

Copy no. ____ of ____ copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date-time group
Message reference number

APPENDIX 2 TO ANNEX B TO OPERATION ORDER (Operation CODE WORD) (U)
SIGNALS INTELLIGENCE

(U) REFERENCES:

(a) Any relevant plans or orders. (Combatant commander, joint task force, or other higher authorities' OPORDs and tactics, techniques, and procedures directives)

(b) Required maps and charts.

(c) (List other documents that provide guidance required for SIGINT and supporting operations planning functions. May include unit SOPs for intelligence and counterintelligence)

1. ( ) Situation. Summarize the overall operational situation as it relates to intelligence operations.

a. ( ) Adversary. (Reference Appendix 11 [Intelligence Estimate] to Annex B. Describe the threat and potential threat, the basic situation, and the SIGINT operations perspective.

CLASSIFICATION

CLASSIFICATION

Identify the enemy's command and control, tactical and electronic orders of battle, and estimates of the enemy's centers of gravity, critical vulnerabilities, intentions, capabilities, and possible courses of action pertinent to SIGINT operations. When possible, identify finished intelligence products supporting these findings. Reference Annex B and current intelligence estimates for threat capabilities, limitations, vulnerabilities, order of battle, and assessed courses of action.)

b. ( ) Friendly. (Reference Annex C [Operations] and other pertinent sources.) Summarize friendly forces situation. Address any critical limitations and any other planned intelligence operations.

c. ( ) Assumptions. List any assumptions made of friendly, adversary, or third-party capabilities, limitations, or courses of action. Describe the conditions the commander believes will exist at the time the plan becomes an order. Omit in orders.

d. ( ) SIGINT Support Available. (Reference Annex A [Task Organization], Annex B, and other pertinent sources. Identify organic, attached, and supporting SIGINT elements available to support MAGTF intelligence operations. Specify elements attached to or in direct support of any subordinate unit.)

2. ( ) Mission. Command's mission from the base order. (Concisely state the SIGINT mission as it relates to the command's planned operation.)

3. ( ) Execution

a. ( ) Concept of SIGINT Support. Summarize how the commander visualizes executing SIGINT operations in support of MAGTF operations. Summarize pertinent command relationships, task organization, main and supporting efforts, and the scope of MAGTF and supporting SIGINT and relevant all-source intelligence operations.

(1) ( ) The concept of support may be a single paragraph or divided into two or more paragraphs depending upon the complexity of the operations.

(2) ( ) When an operation involves various phases, such as peace or pre-hostilities, crisis, war, or post-hostilities, the concept of support should include subparagraphs describing SIGINT support in each phase.

b. ( ) SIGINT Tasks. List and describe tasks to subordinate and attached units (e.g., SIEW support detachment OICs) and requests to higher, adjacent, and cooperating units (e.g., Task Force Commanders).

(1) ( ) RadBn SIEW support detachment CO or OIC.

(2) ( ) Aviation combat element commander.

(3) ( ) Ground combat element (GCE) commander.

CLASSIFICATION

CLASSIFICATION

(4) ( ) Rear area operations center (RAOC) commander.

(5) ( ) (Others as appropriate).

(This section may include direction, requirements, authority, and other guidance regarding SIGINT elements placed in direct support of MAGTF subordinate element. It may also include TSCIFs, SSOs, physical security, and personnel supporting SIGINT and SCI operations, etc.)

c. ( ) Coordinating Instructions. Address any mutual support issues relating to SIGINT operations and requirements. This may include restating MAGTF PIRs; detailed procedures for IR management; SIGINT support requests; direct liaison among subordinate commanders, MAGTF SIGINT units, staff officers, and pertinent external organizations and agencies; routine and time-sensitive reporting and formats; etc.)

4. ( ) Administration and Logistics. Address any SIGINT administrative or logistic requirements.

a. ( ) Logistics. Reference Annex D (Logistics/Combat Service Support). Identify unique combat service support requirements, procedures, and guidance to support MAGTF SIGINT units and operations. Specify procedures for specialized technical logistics support necessary from external organizations (e.g., from DIRNSA or via SCE channels).

b. ( ) Personnel. Reference Annex E (Personnel). Identify SIGINT-unique personnel requirements and concerns, including global sourcing support and contracted linguist requirements.

c. ( ) Consolidated Listing and Impact Assessment of Shortfalls and Limiting Factors. Provide a consolidated listing and impact assessment of personnel and equipment shortfalls and other limiting factors that significantly affect unit SIGINT operations and support. Identify resource problems and specify key tasks that might not be accomplished adequately.

5. ( ) Command and Control. List any SIGINT-related command and control instructions, including pertinent internal and external unit/organization C2 relationships. Identify the command structure for SIGINT operations. Identify any special communications and reporting requirements. Reference the MAGTF’s and SIGINT units’ SOPs and appendix 16 (Intelligence Operations).

a. ( ) Command Relationships. Reference Annex J (Command Relationships). Provide any instructions necessary regarding command relationships and arrangements that will influence MAGTF SIGINT operations, with special attention to C2 relationships concerning SIGINT elements attached to or in direct support of MAGTF subordinate units.

CLASSIFICATION

CLASSIFICATION

b. ( ) Information Management. Reference Annex U (Information Management, Annex C Operations), and Appendix 10 to Annex B (National Intelligence Support Team). Provide any instructions necessary regarding information management (e.g., time sensitive and routine SIGINT reporting criteria, SIGINT data bases, administration and access, and reports) that will influence MAGTF SIGINT operations.

c. ( ) Communications and Information Systems (CIS). Reference Appendix 10 to Annex B (National Intelligence Support Team) and Annex K (Combat Information Systems). Provide any instructions necessary regarding CIS that will influence MAGTF SIGINT operations.

d. ( ) SIGINT C2 Nodes and Facilities. Reference the MAGTF's and SIGINT units' SOPs and Appendix 10 to Annex B (National Intelligence Support Team). Provide any guidance and instructions necessary regarding establishing and operating SIGINT C2 nodes and facilities (e.g., OCAC, amphibious task force ship's signals exploitation spaces) and their integration with other MAGTF C2 nodes (e.g., the MAGTF all-source fusion center, the surveillance and reconnaissance center, the reconnaissance operations center, the amphibious task force intelligence center, electronic warfare coordination center).

ACKNOWLEDGE RECEIPT
Name
Rank and Service
Title

TABS:

A—Communications Intelligence Collection Requirements
B—Operational Electronic Intelligence Collection Requirements

OFFICIAL:

S/
Name
Rank and Service
Title

CLASSIFICATION

CLASSIFICATION
Copy no. ____ of ____ copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date-time group
Message reference number

(U) TAB A TO APPENDIX 2 TO ANNEX B to OPERATION ORDER (Operation CODE WORD)
COMMUNICATION INTELLIGENCE COLLECTION REQUIREMENTS

(U) REFERENCES: Identify plans, documents, maps, and charts essential to effectively creating and executing COMINT collection requirements.

1. ( ) Situation

(The purpose of this tab is to identify operations requirements for COMINT support to the planned MAGTF operation.)

> ***Note:*** SCI controls may require this tab to be published separately from the basic OPORD, Annex B and/or Appendix 2.

a. ( ) General. See basic OPORD. Additionally, orient COMINT collection, processing and exploitation, production, and dissemination efforts to answer the questions listed in paragraphs 2 and 3 below. These requirements should address both organic and external direct support SIGINT resources tasked to support the MAGTF. Reference other pertinent portions of Annex B and current intelligence estimates.

b. ( ) Adversary

(1) ( ) General Capabilities. Identify adversary capabilities directly related to planned SIGINT operations and COMINT collection requirements.

(2) ( ) SIGINT Targets. Describe SIGINT targets anticipated to answer COMINT collection requirements.

(3) ( ) Probable Adversary Course of Action. Refer to Annex B (Intelligence).

c. ( ) Friendly. Summarize the friendly situation, critical limitations, and general SIGINT concept of operations.

d. ( ) Assumptions. List all assumptions upon which COMINT collection requirements are based.

2. ( ) COMINT Collections Requirements and Management

a. ( ) Classification. Designate the overall classification of the information included. Assign the lowest classification possible consistent with established security guidelines.

CLASSIFICATION

CLASSIFICATION

b. ( ) Requirements Statements. Describe, in detail, COMINT information need, priority, specification of timeliness, location accuracy, and periodicity using the following format:

(1) ( ) Requirement. A detailed narrative statement of the requirement.

(2) ( ) Priority. The priority of each requirement specification, using the following criteria for assigning priority:

(a) ( ) Priority 1. Intelligence vital to successful plan implementation (forms the basis for the most crucial operational decisions).

(b) ( ) Priority 2. Intelligence of critical importance to plan implementation, required for making operational decisions and planning future operations.

(c) ( ) Priority 3. Intelligence of major importance to plan implementation, including intelligence required for the security of significant numbers of United States (and allied) forces.

(d) ( ) Priority 4. Intelligence of considerable importance to plan implementation (makes important contribution to operational decision making and planning).

(e) ( ) Priority 5. Intelligence of moderate importance to plan implementation (makes moderate contribution to operational decision making and planning).

(f) ( ) Priority 6. Intelligence of some importance to plan implementation (contributes in a measurable way to operational decision making and planning).

(g) ( ) Priority 7. Intelligence of interest to plan implementation.

(3) ( ) Time. Identify the maximum delay acceptable for receipt of information by the intended user (e.g., within 10 minutes after recognition).

(4) ( ) Location Accuracy. Identify the minimum locational accuracy for which the information is needed (e.g., 95 percent confidence, within 1 kilometer of center mass, within 25 kilometers of emitter location).

(5) ( ) Periodicity. Identify the maximum amount of time that should pass before the target is covered again (i.e., once every 24 hours or once every 8 hours).

c. ( ) User Echelon(s). Identify the primary echelon needing the information (e.g., GCE, RAOC). List multiple users only if all data elements of subparagraph 2.c. above are the same for all listed echelons; otherwise, restate the requirement.

d. ( ) Geographic Area. Specify the geographic area for which the requirement specification applies and defined it precisely (i.e., Country X, 0 to 50 km from western border or Country Y, 50 to 75 km from southeastern border).

CLASSIFICATION

CLASSIFICATION

e. ( ) Justification. For each requirement specification, indicate the operational function(s) or purpose(s) (i.e., artillery targeting or air reconnaissance planning).

3. ( ) Upon OPORD Implementation. List, in the manner described above, the COMINT operational requirements that become relevant upon implementation of the plan. Use subsequent paragraphs to reflect additional support requirements for planned phases of combat operations.

4. ( ) Administration and Logistics. State instructions regarding administrative and logistic support procedures to be used in developing, coordinating, and implementing COMINT collection requirements.

5. ( ) Command and Control. State any specific C2 relationships or special communications or CIS requirements required to support COMINT collection requirements.

(This is not a description of the collection plan but instead focused on collections requirements.)

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

OFFICIAL:

S/
Name
Rank and Service
Title

CLASSIFICATION

APPENDIX E. TEMPORARY SENSITIVE COMPARTMENTED INFORMATION FACILITY CHECKLIST

The following checklist is provided as a guide when activating and deactivating a TSCIF; ensure to consider courier requirements as needed. The security measures identified should be improved upon as the situation permits. Refer to ICD 705, *Sensitive Compartmented Information Facilities* and DODM 5105.21 Volume 1 (dtd 06 Oct 20), *Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information System Security*, for detailed TSCIF operations policy and procedures.

TSCIF ACTIVATION

- ❑ Obtain site location from advance party personnel.
- ❑ Submit request to establish TSCIF to cognizant SSO.
- ❑ Assign vehicle and/or shelter locations to site personnel.
- ❑ Move vehicles into site position. Ensure SCI containers remain locked and guarded until site is accredited.
- ❑ Configure site for operation needs and ease of future movement.
- ❑ Erect shelters, antennas, and camouflage.
- ❑ Establish internal communications (SSO to access control point and emergency reaction force).
- ❑ Review and implement guard procedures.
- ❑ Emplace barrier material and restriction signs.
- ❑ Establish a 24 hour, single gate access point (shelter with lights). Provide guards with access roster of authorized personnel.
- ❑ Determine location of destruction site (burn barrel, etc.).
- ❑ Conduct briefings (i.e., operations security, emergency destruction, emergency evacuation, shift schedule, reaction force, perimeter defense, badge system).
- ❑ Doublecheck physical security of site.
- ❑ Accredit site; declare site secure.
- ❑ Inventory SCI documents and materials as they are unpacked.

- □ Inform G 2/S 2 of commencement of TSCIF operations.
- □ Begin SCI operations and communications.
- □ Send TSCIF activation message.

TSCIF DEACTIVATION

- □ Receive the order to terminate operations.
- □ Coordinate deactivation time with the G 2/S 2.
- □ Zeroize communications security (COMSEC) equipment; ensure message queues are emptied.
- □ Establish guards for SCI materials; inventory and pack SCI into locked containers.
- □ Debrief all one-time access personnel.
- □ Ensure all magnetic media is degaussed a minimum of three times each and all teletype, printers, and/or typewriter ribbons are destroyed or secured with SCI material.
- □ Sweep all SCI work areas for SCI and other classified materials, including telephone directories, newspapers, magazines, notepads, trash bags, etc. Check desk drawers, underneath desks and boxes, equipment containers, bulletin boards, acetate overlays, etc.
- □ Ensure all SCI is either packed in proper containers (IAW DODM 5200.01 Vol 3) for redeployment or destroyed using established procedures.
- □ Account for all TSCIF badges and access rosters.
- □ Make a final inspection of the TSCIF and declare it officially deactivated.
- □ Send TSCIF deactivation message.
- □ Ensure all personnel are briefed on movement time and location and SCI is properly controlled.
- □ Upon termination of operations, return to garrison SCIF, reinventory and account for all SCI material, reset all combination locks, clear all hand receipts, and clean equipment.
- □ Update standing operating procedure and files with lessons learned during the operation.

GLOSSARY SECTION I: ABBREVIATION AND ACRONYMS

AAO	approved acquisition objective
ACE	aviation combat element
AO	area of operations
AOI	area of interest
AOR	area of responsibility
Alt Path	Alternate Path
C2	command and control
CAP	cryptologic augmentation program
CD&I	Combat Development and Integration
CDD	capabilities development document
CDS	cross domain solution
CE	command element
CE-Intel	command element intelligence division
CE-IW	command element information warfare division
CESA	Communications Emitter Sensing and Attack System
CHCSS	Chief, Central Security Service
CI	counterintelligence
CIB	Common Interactive Broadcast
CIS	communications and information system
CMA	collection management authority
CMC	Commandant of the Marine Corps
CMO	collections management officer
CMS	communications security materials system
CNE	computer network exploitation
CO	commanding officer
COMINT	communications intelligence
CPD	capabilities production document
CSG	Cryptologic Support Group
CSS	Central Security Service
C-UAS	counter-unmanned aircraft systems
DC/S	Deputy Chief of Staff
DF	direction finding
DIA	Defense Intelligence Agency
DIRINT	Director of Intelligence
DIRNSA	Director, National Security Agency
DNI	Director of National Intelligence
DOA	direction of arrival
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction
DODIIS	Department of Defense Intelligence Information System

DODIN	Department of Defense information network
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy
DS	direct support
DST	direct support team

EA	electromagnetic attack
ELINT	electronic intelligence
EMS	electromagnetic spectrum
EO	executive order
EP	electromagnetic protection
ES	electromagnetic support
EW	electromagnetic warfare
EWS	electronic warfare systems
EWSA	electronic warfare services architecture

FDOA	frequency difference of arrival
FISINT	foreign instrumentation signals intelligence
FoS	Family of Systems

G-1	assistant chief of staff, personnel/personnel staff section
G-2	assistant chief of staff, intelligence/intelligence staff section
G-3	assistant chief of staff, operations and training/operations and training staff section
G-4	assistant chief of staff, logistics/logistics staff section
G-5	assistant chief of staff, plans/plans staff section
G-6	assistant chief of staff, communications/communications system staff section
GCE	ground combat element
GENSER	general service (message)
GEOINT	geospatial intelligence
GS	general support
GSA	General Services Administration

HF	high frequency
HQMC	Headquarters, United States Marine Corps
HUMINT	human resources intelligence

I&W	indications and warnings
IA	information assurance
IBR	intelligence broadcast receiver
IBS	integrated broadcast service
IC	intelligence community
ICD	intelligence community directive
ICR	intelligence collection requirement
I-EMO	Intelligence-Enterprise Management Officer
IID	Intelligence Integration Division
IMA	individual mobilization augmentee
Intel	intelligence

IO	information operations
IOC	intelligence operations center
IOO	Intelligence Operations Officer
IR	intelligence requirement
IT	information technology
IT II	Intrepid Tiger II
JCIDS	Joint Capabilities Integration and Development System
JEON	joint emergent operational need
JP	joint publication
JROC	joint requirements oversight council
JTF	joint task force
JUON	joint urgent operational need
JWICS	Joint Worldwide Intelligence Communications System
LAN	local area network
LAV	light armored vehicle
LCE	logistic combat element
LOB	line of bearing
LOS	line of sight
LTI	limited technical inspection
M&RA	Manpower and Reserve Affairs (HQMC)
MAGTF	Marine air-ground task force
MARCORSYSCOM	Marine Corps Systems Command
MARDIV	Marine division
MARFOR	Marine Forces
MARFORCOM	Marine Forces Command
MARFORCYBERCOM	Marine Forces Cyberspace Command
MARFORPAC	Marine Corps Forces Pacific
MARSOC	Marine Special Operations Command
MASINT	measurement and signature intelligence
MAW	Marine aircraft wing
MAWTS-1	Marine Aviation Weapons and Tactics Squadron One
MCCDC	Marine Corps Combat Development Command
MCIA	Marine Corps Intelligence Activity
MCIS	Marine Corps Intelligence Schools
MCISRE	Marine Corps Intelligence, Surveillance, and Reconnaissance Enterprise
MCLOG	Marine Corps Logistics and Operations Group
MCSB	Marine Cryptologic Support Battalion
MCSE	Marine Cryptologic Support Element
MCSIL	Marine Corps Spectrum Integration Laboratory
MEB	Marine expeditionary brigade
MEF	Marine expeditionary force
MEU	Marine expeditionary unit
MHz	megahertz
MIC	MAGTF Intelligence Center

MIG	Marine expeditionary force information group
MIP	military intelligence program
MOS	military occupational specialty
MSC	major subordinate command

NCR	National Security Agency/Central Security Service Representative
NCW	Non-code word
NDA	Nondisclosure Agreement
NIP	National Intelligence Program
NNWC	Naval Network Warfare Command
NOC	network operations center
NRT	near real time
NS	network services
NSA	National Security Agency
NSANet	National Security Agency Network
NSCID	National Security Council Intelligence Directive
NTI	National-to-Tactical Integration

OCA	operations control and analysis
OCAC	operations control and analysis center
OCE	operations control element
ODNI	Office of the Director of National Intelligence
OIC	officer in charge
OPCON	operational control
OPELINT	operational electronic intelligence
OPORD	operations order
OSD	Office of the Secretary of Defense

PGL	precision geolocation
PIR	priority intelligence requirement
POM	program objective memorandum
PoR	Program of Record
PTP	predeployment training program

R&S	Reconnaissance and Surveillance
RadBn	radio battalion
RAWS	Remote Analysis Workstations
RDT&E	research, development, test, and evaluation
RF	radio frequency
RP&G	reporting policy and guidance
RREP	radio reconnaissance equipment program
RRT	radio reconnaissance team
RTP	requirements transition process

S-1	personnel officer/personnel office
S-2	intelligence officer/intelligence office
S-3	operations and training officer/operations and training office

S-4	logistics officer/logistics office
S-6	communications system officer/communications staff office
SATCOM	satellite communications
SCC	service cryptologic component
SCE	service cryptologic element
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SecDef	Secretary of Defense
SIEW	signals intelligence and electromagnetic warfare
SIGINT	signals intelligence
SIGMAN	signature management
SIO	signals intelligence officer
SIPRNET	SECRET Internet Protocol Router Network
SOI	signal of interest
SOTA	signals intelligence operational tasking authority
SPC	Signals intelligence production chain
SS	SIGINT Suite
SSES	ship’s signal exploitation space
SSF	Spectrum Services Framework
SSO	special security officer
SST	signals intelligence support team
SVPT	SIGMAN Visualization Planning Tool

T/E	table of equipment
T/O	table of organization
TCAC	technical control and analysis center
TECHCON	technical control
TECHELINT	technical electronic intelligence
TECHINT	technical intelligence
TECOM	Training and Education Command
TNG	Theater Net-centric Geolocation
TPCS	team portable collection system
TPCS-MPC	team portable collection system-multi-platform capable
TSCIF	temporary sensitive compartmented information facility
TSCS	tactical SIGINT collection systems
TTP	tactics, techniques, and procedures
TWS	transportable workstation

UHF	ultrahigh frequency
UNS	universal needs statements
UON	urgent operational need
USD(I)	Under Secretary of Defense for Intelligence
USMC	United States Marine Corps
USSID	United States signals intelligence directive
USSOCOM	United States Special Operations Command
USSS	United States Signals Intelligence System
UUNS	urgent universal needs statements

VHF	very high frequency
VTC	video teleconferencing
WTI	weapons and tactics instructor

GLOSSARY SECTION II. TERMS AND DEFINITIONS

all-source intelligence

Intelligence products and/or organizations and activities that incorporate all sources of information in the production of finished intelligence. (DOD Dictionary, part 1 of a 2-part definition)

amphibious objective area

A geographical area of sufficient size for conducting necessary sea, air, and land operations and within which is located the objective(s) to be secured by the amphibious force. Also called **AOA**. (DOD Dictionary)

area of interest

That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory. Also called **AOI**. (DOD Dictionary)

area of operations

An operational area defined by a commander for land and maritime forces that should be large enough to accomplish their missions and protect their forces. Also called **AO**. (DOD Dictionary)

battle damage assessment

(See DOD Dictionary for core definition. Marine Corps amplification follows.) The timely and accurate estimate of the damage resulting from the application of military force. Battle damage assessment estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. Also called **BDA**. (USMC Dictionary)

battlespace

The environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, and/or complete the mission. It includes the physical environment (air, land, maritime, and space domains); the information environment (which includes cyberspace); the electromagnetic spectrum; and other factors. Included within these are friendly, enemy, adversary, and neutral entities contained within or having an effect on the operational areas, areas of interest, and areas of influence. (USMC Dictionary)

battlespace dominance

The degree of control over the dimensions of the battlespace that enhances friendly freedom of action and denies enemy freedom of action. It permits force sustainment and application of power projection to accomplish the full range of potential operational and tactical missions. It includes all actions conducted against enemy capabilities to influence future operations. (USMC Dictionary)

centralized control

(See DOD Dictionary for core definition. Marine Corps amplification follows.) In military operations, a mode of battlespace management in which one echelon of command exercises total authority and direction of all aspects of one or more warfighting functions. It is a method of control where detailed orders are issued and total unity of action is the overriding consideration. (USMC Dictionary)

collection

(See DOD Dictionary for core definition. Marine Corps amplification follows.) The gathering of intelligence data and information to satisfy the identified requirements. (USMC Dictionary)

collection management

In intelligence usage, the process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results and retasking, as required. (DOD Dictionary)

combat data

Data derived from reporting by operational units. (USMC Dictionary)

combatant command

A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Also called **CCMD**. (DOD Dictionary)

command and control

(See DOD Dictionary for core definition. Marine Corps amplification follows.) The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. Command and control is one of the seven warfighting functions. Also called **C2**. (USMC Dictionary)

commander's critical information requirements

(See DOD Dictionary for core definition. Marine Corps amplification follows.) Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decision-making. Also called **CCIR**. (USMC Dictionary)

commander's intent

(See DOD Dictionary for core definition. Marine Corps amplification follows.) A commander's clear, concise articulation of the purpose(s) behind one or more tasks assigned to a subordinate. It is one of two parts of every mission statement that guides the exercise of initiative in the absence of instructions. (USMC Dictionary)

communications intelligence

Technical information and intelligence derived from foreign communications by other than the intended recipients. Also called **COMINT**. (DOD Dictionary)

communications security

Actions designed to deny unauthorized persons information of value by safeguarding access to, or observation of, equipment, material, and documents with regard to the possession and study of telecommunications or to purposely mislead unauthorized persons in their interpretation of the results of such possession and study. Also called **COMSEC**. (DOD Dictionary)

coordination

The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as fire support, emergency defense measures, area intelligence, and other situations in which coordination is considered necessary. (USMC Dictionary)

critical information

Specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (DOD Dictionary)

critical intelligence

Intelligence that is crucial and requires the immediate attention of the commander. (DOD Dictionary)

critical vulnerability

(See DOD Dictionary for core definition. Marine Corps amplification follows.) An aspect of a center of gravity that if exploited, will do the most significant damage to an enemy's and/or adversary's ability to resist. A vulnerability cannot be critical unless it undermines a key strength. Also called **CV**. (USMC Dictionary)

decentralized control

(See DOD Dictionary for core definition. Marine Corps amplification follows.) In military operations, a mode of battlespace management in which a command echelon may delegate some or all authority and direction for warfighting functions to subordinates. It requires careful and clear articulation of mission, intent, and main effort to unify efforts of subordinate leaders. (USMC Dictionary)

descriptive intelligence

Class of intelligence that describes existing and previously existing conditions with the intent to promote situational awareness. Descriptive intelligence has two components: basic intelligence, which is general background knowledge about established and relatively constant conditions; and current intelligence, which is concerned with describing the existing situation. (USMC Dictionary)

detachment

1. A part of a unit separated from its main organization for duty elsewhere. 2. A temporary military or naval unit formed from other units or parts of units. Also called **Det**. (USMC Dictionary)

direction finding

A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment. Also called **DF**. (DOD Dictionary)

dissemination

(See DOD Dictionary for core definition. Marine Corps amplification follows.) Conveyance of intelligence to users in a suitable form. (USMC Dictionary)

electromagnetic attack

Division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. Also called **EA**. (DOD Dictionary)

electromagnetic protection

Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. Also called **EP**. (DOD Dictionary)

electromagnetic support

Division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Also called **ES**. (DOD Dictionary)

electromagnetic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called **EW**. DOD Dictionary)

electronic intelligence

Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called **ELINT**. (DOD Dictionary)

essential elements of friendly information

(See DOD Dictionary for core definition. Marine Corps amplification follows.) Specific facts about friendly intentions, capabilities, and activities needed by enemies and adversaries to plan and execute effective operations against our forces. Also called **EEFI**. (USMC Dictionary)

estimative intelligence

(See DOD Dictionary for core definition. Marine Corps amplification follows.) Class of intelligence that attempts to anticipate future possibilities and probabilities based on an analysis of descriptive intelligence in the context of planned friendly and assessed enemy operations. (USMC Dictionary)

friendly force information requirements

(See DOD Dictionary for core definition. Marine Corps amplification follows.) Information the commander needs about friendly forces in order to develop plans and make effective decisions. Depending upon the circumstances, information on unit location, composition, readiness, personnel status, and logistics status could become a friendly force information requirement. Also called **FFIR**. (USMC Dictionary)

fusion

In intelligence usage, the process of managing information to conduct all-source analysis and derive a complete assessment of activity. (DOD Dictionary)

global sourcing

A process of force provision or augmentation whereby resources may be drawn from any location/ command worldwide. (USMC Dictionary)

indications and warning

Those intelligence activities intended to detect and report time sensitive intelligence information on foreign developments that could involve a threat to the United States or allied and/or coalition military, political, or economic interests or to United States citizens abroad. It includes forewarning of hostile actions or intentions against the United States, its activities, overseas forces, or allied and/or coalition nations. Also called **I&W**. (USMC Dictionary)

intelligence

(See DOD Dictionary for core definition. Marine Corps amplification follows.) Knowledge about the enemy or the surrounding environment needed to support decision making. Intelligence is one of the seven warfighting functions. (USMC Dictionary)

intelligence cycle

A six-step process by which information is converted into intelligence and made available to users. The six steps are planning and direction, collection, processing and exploitation, production, dissemination, and utilization. (USMC Dictionary)

intelligence data

Data derived from assets primarily dedicated to intelligence collection such as imagery systems, electronic intercept equipment, human intelligence sources, etc. (USMC Dictionary)

intelligence discipline

A well defined area of intelligence planning, collection, processing, exploitation, analysis, and reporting using a specific category of technical or human resources. (DOD Dictionary)

intelligence operations

The variety of intelligence and counterintelligence tasks that are carried out by various intelligence organizations and activities within the intelligence process. (DOD Dictionary)

intelligence preparation of the battlespace

(See DOD Dictionary for core definition. Marine Corps amplification follows.) The systematic, continuous process of analyzing the threat and environment in a specific geographic area. Also called **IPB**. (USMC Dictionary)

intelligence requirement

(See DOD Dictionary for core definition. Marine Corps amplification follows.) Questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. Also called **IR**. (USMC Dictionary)

irregular warfare

A violent struggle among state and non-state actors for legitimacy and influence over the relevant population(s). Also called **IW**. (DOD Dictionary)

joint deployable intelligence support system

A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. Also called **JDISS**. (DOD Dictionary)

joint force

A force composed of elements, assigned or attached, of two or more Military Departments operating under a single joint force commander. (DOD Dictionary)

Joint Worldwide Intelligence Communications System

The sensitive compartmented information portion of the Defense Information System Network, which incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called **JWICS**. (DOD Dictionary)

main effort

The designated subordinate unit whose mission at a given point in time is most critical to overall mission success. It is usually weighted with the preponderance of combat power and is directed against a center of gravity through a critical vulnerability. (USMC Dictionary)

maneuver warfare

A warfighting philosophy that seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions that create a turbulent and rapidly deteriorating situation with which the enemy cannot cope. (USMC Dictionary)

Marine Corps Planning Process

A six-step methodology that helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the mission and the threat and is based on the Marine Corps philosophy of maneuver warfare. It capitalizes on the principle of unity of command and supports the establishment and maintenance of tempo. The six steps consist of problem framing, course of action development, course of action wargame, course of action comparison and decision, orders development, and transition. Also called **MCPP**. (Note: Tenets of the MCPP include top down planning, single battle concept, and integrated planning.) (USMC Dictionary)

named area of interest

(See DOD Dictionary for core definition. Marine Corps amplification follows.) A point or area along a particular avenue of approach through which enemy activity is expected to occur. Activity or lack of activity within a named area of interest will help to confirm or deny a particular enemy course of action. Also called **NAI**. (USMC Dictionary)

network engagement

Interactions with friendly, neutral, and threat networks, conducted continuously and simultaneously at the tactical, operational, and strategic levels, to help achieve the commander's objectives within an operational area. (DOD Dictionary)

operational architecture

1. Description of the tasks, operational elements, and information flows required to accomplish or support a warfighting function. 2. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanges. (USMC Dictionary)

operational control

(See DOD Dictionary for core definition. Marine Corps amplification follows.) With respect to a flight, the exercise of authority over initiating, conducting, or terminating a flight. Also called **OPCON**. (USMC Dictionary)

operations control and analysis center

Main node for the command and control of radio battalion signals intelligence operations and the overall coordination of Marine air-ground task force signals intelligence operations. The center processes, analyzes, produces, and disseminates signals intelligence derived information and directs the ground based electronic warfare activities of the radio battalion. Also called **OCAC**. (USMC Dictionary)

order of battle

The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. Also called **OB**; **OOB**. (DOD Dictionary)

priority intelligence requirements

(See DOD Dictionary for core definition. Marine Corps amplification follows.) An intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. Also called **PIR**. (USMC Dictionary)

production management

Encompasses determining the scope, content, and format of each intelligence product; developing a plan and schedule for the development of each product; assigning priorities among the various production requirements; allocating processing, exploitation, and production resources; and integrating production efforts with intelligence collection and dissemination. (USMC Dictionary)

reachback

(See DOD Dictionary for core definition. Marine Corps amplification follows.) The ability to exploit resources, capabilities, expertise, etc., not physically located in the theater or a joint operations area, when established. (USMC Dictionary)

sensitive compartmented information

All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. (Note: These controls are over and above the provisions of DODM 5200.01, DOD Information Security Program.) Also called **SCI**. (DOD Dictionary)

sensitive compartmented information facility

An accredited area, room, group of rooms, or installation where sensitive compartmented information may be stored, used, discussed, and/or electronically processed, where procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular sensitive compartmented information authorized for use or storage within the sensitive compartmented information facility. Also called **SCIF**. (DOD Dictionary)

sensor data

Data derived from sensors whose primary mission is surveillance or target acquisition, such as air surveillance radar, counterbattery radar, and remote ground sensors. (USMC Dictionary)

Service component command

A command consisting of the Service component commander and all those Service forces, such as individuals, units, detachments, organizations, and installations under the command, including the support forces that have been assigned to a combatant command or further assigned to a subordinate unified command or joint task force. (DOD Dictionary)

signals intelligence

1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted.
2. Intelligence derived from communications, electronic, and foreign instrumentation signals. Also called **SIGINT**. (DOD Dictionary)

signals intelligence operational tasking authority

A military commander’s authority to operationally direct and levy signals intelligence requirements on designated signals intelligence resources; includes authority to deploy and redeploy all or part of the signals intelligence resources for which signals intelligence operational tasking authority has been delegated. Also called **SOTA**. (Note: Also see USSID 1, SIGINT Operating Policy) (DOD Dictionary)

situational awareness

Knowledge and understanding of the current situation that promotes timely, relevant, and accurate assessment of friendly, enemy, and other operations within the battlespace in order to facilitate decision making. An informational perspective and skill that foster an ability to determine quickly the context and relevance of events that are unfolding. Also called **SA**. (USMC Dictionary)

split base

Two or more portions of the same force conducting or supporting operations from separate physical locations. (USMC Dictionary)

surveillance and reconnaissance cell

Primary element responsible for the supervision of Marine air-ground task force intelligence collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets. Also called **SARC**. (USMC Dictionary)

sustained operations ashore

The employment of Marine Corps forces on land for an extended duration. It can occur with or without sustainment from the sea. Also called **SOA**. (USMC Dictionary)

systems architecture

Defines the physical connection, location, and identification of key nodes, circuits, networks, warfighting platforms, etc., and specifies system and component performance parameters. The systems architecture is constructed to satisfy operational architecture requirements per standards defined in the technical architecture. The systems architecture shows how multiple systems within a subject area link and interoperate, and it may describe the internal construction or operations of particular systems within the architecture. (USMC Dictionary)

tactical intelligence

(See DOD Dictionary for core definition. Marine Corps amplification follows.) Intelligence concerned primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and the tactical aspects of terrain and weather within the battlespace. (USMC Dictionary)

technical architecture

A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. Identifies the services, interfaces, standards, and their relationships and provides the technical guidelines to implement systems upon which engineering specifications are based, common building blocks are built, and product lines are developed. (USMC Dictionary)

technical control

The performance of specialized/professional service or the exercise of professional guidance/direction through the establishment of policies and procedures. Also called **TECHCON**. (USMC Dictionary)

tempo

The relative speed and rhythm of military operations over time with respect to the enemy. (USMC Dictionary)

warfighting functions

The seven mutually supporting military activities integrated in the conduct of all military operations. The seven warfighting functions are command and control, fires, force protection, information, intelligence, logistics, and maneuver. (USMC Dictionary)

REFERENCES AND RELATED PUBLICATIONS

Federal Issuance

Executive Order 12333 United States Intelligence Activities

Department of Defense Issuances

Department of Defense Directives (DODDs)

5100.20	National Security Agency/Central Security Service (NSA/CSS)
TS-5105.21-M-2	Sensitive Compartmented Information (SCI) Security Manual, Communications Intelligence (COMINT) Policy
TS-5105.21-M-3	Sensitive Compartmented Information (SCI) Security Manual, TK Policy

Department of Defense Instructions (DODIs)

3305.09	DOD Cryptologic Training
O-3115.07	Signals Intelligence
5200.01	DOD Information Security Program and Protection of Sensitive Compartmented Information (SCI)

Department of Defense Manuals (DODMs)

5105.21, Vol 1	Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security
5200.01, Vol 1	DOD Information Security Program: Overview, Classification, and Declassification
5200.01, Vol 3	DOD Information Security Program: Protection of Classified Information
S-5240.01-A	(U) Procedures Governing the Conduct of DOD Intelligence Activities: Annex Governing Signals Intelligence Information and Data Collected Pursuant to Section 1.7(c) of EO 12333

Director of National Intelligence Community Directives (ICDs)

503	Intelligence Community Information Technology Systems Security Risk Management
703	Protection of Classified National Intelligence, Including SCI
704	Personnel Security
705	Sensitive Compartmented Information Facilities

United States Signals Intelligence Directive (USSIDs)

1	SIGINT Operating Policy
4	Concept of SIGINT Support to Military Commanders
18	Legal Compliance and US Persons Minimization Procedures
56	Exercise SIGINT

200	Technical SIGINT Reporting
240	ELINT Processing, Analysis, Reporting, and Forwarding Procedures
300	SIGINT Reporting
316	Non-Codeword Reporting Program
340	Tactical ELINT Reporting
341	Technical ELINT Reporting
510	Information for SIGINT Users

Defense Intelligence Agency Directive (DIAD)

8500.200	DOD SCI and DODIIS Community Cyber Security Programs

Defense Intelligence Agency Instruction (DIAI)

8500.001	DOD SCI and DODIIS Community Cyber Security Programs

Secretary of the Navy Instruction (SECNAVINST)

5510.30C	Department of the Navy Personnel Security Program

Miscellaneous

Department of Defense Dictionary of Military and Associated Terms

Joint Issuances

Joint Publications (JPs)

2-0	Joint Intelligence
2-01	Joint and National Intelligence Support to Military Operations
3-02	Amphibious Operations
3-13.3	Operations Security
5-0	Joint Planning
6-0	Joint Communications System

Miscellaneous

Joint Tactical Exploitation of National Systems (J-TENS) Manual

Marine Corps Publications

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
2	Intelligence
3	Expeditionary Operations
4	Logistics
5	Planning
6	Command and Control
7	Learning

Marine Corps Warfighting Publications (MCWPs)

2-10	Intelligence Operations
5-10	Marine Corps Planning Process

Marine Corps Tactical Publication (MCTP)

3-02A	MAGTF Network Engagement Activities.

Marine Corps Reference Publication (MCRP)

1-10.1	Organization of Marine Corps Forces
3-32D.1	Electronic Warfare

Marine Corps Orders (MCOs)

3500.41 w/Erratum	Signals Intelligence Training and Readiness Manual
5500.6H CH 1	Arming of Law Enforcement and Security Personnel and the Use of Force

Miscellaneous

Marine Corps Supplement to the DOD Dictionary of Military and Associated Terms.

Army Publications

Army Techniques Publications (ATPs)

2-01	Plan Requirements and Assess Collection
2-01.3	Intelligence Preparation of the Battlefield
2-22.6	Signals Intelligence Techniques (TS)
2-22.6-2	Signals Intelligence Volume II: Reference Guide

Army Field Manuals (FMs)

2-0	Intelligence

Copyright Information