

# Security and Emergency Services Community of Interest

---



0080 – Security Administration Series

(Mission Assurance)

Career Road Map & Training Strategy

## Overview of the 0080 Mission Assurance Career Road Map and Training Strategy

The United States Marine Corps (USMC) Security and Emergency Services (S&ES) Community of Interest (COI) developed this career road map and training strategy to support 0080-Security Administration (Mission Assurance (MA) focus) series professional development of technical competencies and training. This learning map is organized by a group of competencies, which together define successful performance in the 0080-Security Administration (MA) series. Career road maps combined with a training strategy are essential resources for career development and useful for identifying the knowledge and skillsets needed to meet and/or enhance their skills in this occupational series.

This competency-based career road map was developed based on guidance from the Office of Personnel Management (OPM) Position Classification Standard, OPM Grade Evaluation Guide and via working groups using 0080 leaders across the USMC.

Career road maps are comprised of several components, described in Table 1 below:

**Table 1. Components of a Career Road Map and Training Strategy**

<b>Competency Titles and Definitions</b>	Describe the capabilities required within a position or job role.
<b>Proficiency Targets</b>	Define different levels of required performance (Intermediate, Supervisor and Expert/Senior Management) within a competency area.
<b>Behavioral Indicators (BIs)</b>	Examples of activities performed by an individual that illustrate how a competency is demonstrated at varying levels of proficiency: Intermediate, Supervisor and Expert/Senior Management.
<b>Career Progression</b>	<ul style="list-style-type: none"> <li>• <b>Career Paths and Progression:</b> Provides employee with examples of the various career paths and progression from entry level employee to management level.</li> </ul>
<b>Training</b>	<ul style="list-style-type: none"> <li>• <b>Core:</b> Initial training that all personnel should have in related position from entry to senior levels.</li> <li>• <b>Core-Plus/Leadership:</b> Advanced and leadership training that is necessary for career progression that is recommended for mid-senior personnel in addition to core training.</li> <li>• <b>Career Enhancing/Sustainment:</b> Training intended to maintain credentials or a good training course to have, but not necessary for career advancement.</li> </ul>

## Security Administration Series Defined

---

This series includes positions the primary duties of which are analytical, planning, advisory, operational, or evaluative work that has as its principal purpose the development and implementation of policies, procedures, standards, training, and methods for identifying and protecting missions, critical infrastructure, information, personnel, property, facilities, operations, or material from unauthorized disclosure, misuse, theft, assault, vandalism, espionage, sabotage, or loss. Duties involve the management, supervision, or performance of work in: (1) developing, evaluating, maintaining, and/or operating systems, policies, devices, procedures, and methods used for safeguarding information, property, personnel, operations, and materials; and/or (2) developing and implementing policies and procedures for analyzing and evaluating the character, background, and history of employees, candidates for employment, and other persons having or proposed to be granted access to classified or other sensitive information, materials, or work sites.

## Competency Areas

---

Four competencies have been identified for the successful performance in the 0080-Security Administration (MA) series:

1. Mission Assurance
2. Critical Infrastructure Protection
3. Mission Assurance Risk Management
4. Protection Program Management

## Proficiency and Skill Band Definitions

---

The Proficiency Rating Scale (Table 2) below details the rating given for each level of proficiency and its corresponding definition. Proficiency levels describe the degree of competency required to perform a specific job successfully; these levels relate to the work required for a specific job. Different jobs require different levels of proficiency for successful performance. The proficiency levels provided in this learning map indicate the minimum proficiency target for successful performance.

**Table 2. Proficiency Rating Scale**

<b>1</b>	<b>Basic</b>	No Proficiency	Conceptual Knowledge Only/No Experience
<b>2</b>	<b>Applied</b>	Low Proficiency	Able to Apply with Help
<b>3</b>	<b>Intermediate</b>	Moderate Proficiency	Able to Apply Autonomously
<b>4</b>	<b>Advanced</b>	High Proficiency	Proficient/Able to Help Others
<b>5</b>	<b>Expert</b>	Very High Proficiency	Expert Knowledge

The USMC COI has outlined a career progression structure that more accurately reflects the change in your abilities and responsibilities over time. That structure is called the Skill Level Structure (Table 3). It is associated with each occupational series and follows you from the time you are an entry-level employee until you attain the level of a management employee. Career progress in the USMC has traditionally been based on the federal government pay schedule system. The ratings within the pay schedule system are associated with Job Skill Levels within the 0080-Security Administration series indicated as follows:

**Table 3. Skill Level Structure**

Job Skill Level	Definition	Job Titles Within Skill Levels	Pay Plan	Beginning Grade	Target Grade
3	Intermediate	Mission Assurance Specialist/Critical Infrastructure Analyst	GS	10	12
4	Advanced	Mission Assurance Specialist/Critical Infrastructure Analyst	GS	12	13
4/5	Supervisor	Mission Assurance Program Manager	GS	13	14
5	Management	Mission Assurance Section/Department Head	GS	14	15

**Advancing Levels of Expertise within the 0080-Security Administration Series**

Level 3	Level 4	Level 4	Level 5
Intermediate Level (GS 10-12)	Advanced (GS 12-13)	Supervisory (GS 13-14)	Management (GS-14-15)
<p>At the intermediate level, incumbent is responsible for performing many tasks with moderate proficiency and some direct supervision.</p>	<p>At the advanced level, the incumbent is responsible for applying knowledge and understanding of relevant laws, policy and regulations; performing duties and responsibilities without direct supervision.</p>	<p>At the expert level, the incumbent is responsible for managing the work and activities of junior security specialists and possessing advanced knowledge and understanding of relevant laws and regulations; directs project and/or program activities.</p>	<p>At the management level, the incumbent is responsible for managing the work and activities of analysts and supervisors; possess expert knowledge and understanding of relevant laws and regulations; directs project and/or program activities.</p>
<p><b>Desired Academic Credentials</b> High School Graduate</p>	<p><b>Desired Academic Credentials</b> Any BA/BS Degree</p>	<p><b>Desired Academic Credentials</b> Any BA/BS Degree</p>	<p><b>Desired Academic Credentials</b> Any Advanced Degree</p>
<p><b>Experience</b> 1 year of specialized experience equivalent to the GS 10 level where work is in or directly related to the line of work of the position.</p>	<p><b>Experience</b> 1 year of specialized experience equivalent to the GS -12 level where work is in or directly related to the line of work of the position.</p>	<p><b>Experience</b> 1 year of specialized experience equivalent to the GS-13 level where work is in or directly related to the line of work of the position.</p>	<p><b>Experience</b> 1 year of specialized experience equivalent to the GS-14 level where work is in or directly related to the line of work of the position.</p>
<p><b>Training: CORE</b> See Table 5</p>	<p><b>Training: Core</b> See Table 5</p> <p><b>Core Plus/ Leadership</b> See Table 6</p> <p><b>Position Specific Specialized Training</b> See Table 7</p>	<p><b>Training: Core</b> See Table 5</p> <p><b>Core Plus/ Leadership</b> See Table 6</p> <p><b>Position Specific Specialized Training</b> See Table 7</p>	<p><b>Training: Core</b> See Table 5</p> <p><b>Core Plus/Leadership</b> See Table 6</p> <p><b>Position Specific Specialized Training</b> See Table 7</p>

## Career Progression

---

The 0080-Security Administration Series has various career paths and progression for the intermediate level to consider as they move through the job skill levels: entry, journeyman, supervisory and management. Table 4 provides examples of career paths and progression available to them. The following table provides *examples of* career path and progression in the 0080- Security Administration Series:

**Table 4. Career Path Progression Examples**

Intermediate	Advanced	Supervisory	Management
GS 10-12	GS 12 - 13	GS 13-14	GS 14 - 15
Specialist/Analyst	Manager/Supervisor	Manager	Section/Department Head

## Behavioral Indicators (BIs)

---

It is important to define how competencies are manifested at different skill levels. Behavioral Indicators are on-the-job examples of behaviors and activities that illustrate how a competency is demonstrated at varying skill levels and provide an objective description of the behavior that can be observed in an individual as evidence that they either have or do not have the skills at the required level needed for the competency. These are examples of what the competency could look like at varying skill levels and are not inclusive of all behaviors demonstrating the competency for each skill level. This information is provided as a tool to help guide evaluations of employee proficiency; however, it should not be used as a checklist for employees' behaviors.

## Training

---

Tables 5-8 define the Core, Core-Plus/Leadership, Position Specific Training and Advanced/Career Enhancement training courses within the 0080-Security Administration (MA) series. Training is aligned to job roles and grade levels. Training titles and vendors are subject to change as the courses evolve. Additionally, there are several external resources (DoD, local, state and commercial) that provide a variety of training opportunities available to all USMC civilian personnel for professional knowledge and skill development. Individuals are to work with their supervisor for approved training courses available to them. These training lists are to be used as a guide for professional development purposes and are only provided as a recommendation and may not encompass all training available to the 0080- Security Administration (MA) series. Individuals are to work with supervisors to determine the best training courses suited for each position and for career progression.

**Table 5. Core Training by Job Role**

Core Training	Notes	Vendor	Mission Assurance Specialist (GS 10-12)	Critical Infrastructure Analyst (GS 10-12)	Mission Assurance Program Manager (GS 13 /14)	Mission Assurance Supervisor (GS 13/14)	Mission Assurance Manager (GS 14/15)
Antiterrorism Level I Awareness		DOD	●	●	●	●	
Antiterrorism Level II Course		MarineNet	●	●	●	●	
MARMGMT001 Marine Corps Mission Assurance Risk Management		MarineNet	●	●	●	●	
DI5500A Critical Infrastructure Protection (CIP): Beginning the CIP Process		MarineNet	●	●	●	●	
DI5500B Critical Infrastructure Protection (CIP): CIP Remediation		MarineNet	●	●	●	●	
DI5500C Critical Infrastructure Protection (CIP): Reacting to Potential Threats		MarineNet	●	●	●	●	
DI5500D Critical Infrastructure Protection (CIP): Consequence Management Planning		MarineNet	●	●	●	●	
M00CIP0799 Critical Infrastructure Protection		MarineNet	●	●	●	●	
DI55000ZZ Department of the Navy, Critical Infrastructure Protection (CIP) Program Curriculum		MarineNet	●	●	●	●	
MACIPB0001 Critical Infrastructure Program (CIP) Basics		MarineNet	●	●	●	●	

*\*Initial training that all personnel should have in related position from entry to senior levels.*

**Table 6. Core Plus/Leadership Training by Job Role**

Core Plus / Leadership Training	Notes	Vendor	Mission Assurance Specialist (GS 10-12)	Critical Infrastructure Analyst (GS 10-12)	Mission Assurance Program Manager (GS 13 /14)	Mission Assurance Supervisor (GS 13/14)	Mission Assurance Manager (GS 14/15)
Critical Infrastructure Security and Resilience Awareness AWR213		TEEX	●	●	●	●	●
Understanding Targeted Cyber Attacks AWR376		TEEX			●	●	●
Terrorist Attack Style LET711		TEEX			●	●	●
Advanced Critical Infrastructure Protection MGT414		TEEX			●	●	●
Physical and Cyber Security for Critical Infrastructure MGT452		TEEX			●	●	●
Critical Infrastructure Security and Resilience Awareness AWR213		TEEX			●	●	●
Understanding Targeted Cyber Attacks AWR376		TEEX			●	●	●
Terrorist Attack Style LET711		TEEX			●	●	●
Advanced Critical Infrastructure Protection MGT414		TEEX			●	●	●
Civilian Career and Leadership Development (CCLS)		DOD			●	●	●
Marine Corps Civilian Leadership Development Program (MCCLDP)		DOD			●	●	●
Administrative Officers Course		DOD	●	●	●	●	●



**Table 7. Advanced Training (Career Enhancing) by Job Role**

Advanced Training (Career Enhancing)	Notes	Vendor	Mission Assurance Specialist (GS 10-12)	Critical Infrastructure Analyst (GS 10-12)	Mission Assurance Program Manager (GS 13 /14)	Mission Assurance Supervisor (GS 13/14)	Mission Assurance Manager (GS 14/15)
Project Management Professional Course		Commercial			•	•	•
Policy and Budget Execution Course		DOD		•	•	•	•
Training for Accountable Officials and Certifying Officers		DTMO		•	•	•	•
USMC E-ITSM ITPRAS Submitter Course ITSM14IS01		USMC		•	•	•	•

*\*\*Core Plus/leadership training that is necessary for career progression from intermediate level through management*

## Competency Model

---

COMPETENCY	DEFINITION			
<p><b>1. Mission Assurance</b></p>	<p>Uses knowledge of mission assurance to execute the process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DoD mission-essential functions in any operating environment or condition. Coordinates the Mission Assurance Related Program Activities (MARPA); Adaptive Planning, Antiterrorism, CBRN Survivability, CBRNE Preparedness, Continuity of Operations (COOP), Cybersecurity, Defense Critical Infrastructure, Emergency Management, Energy Resilience, Fire Prevention and Protection, Force Health Protection, Insider Threat, Law Enforcement, Operations Risk Management, Operational Energy, Readiness Reporting,</p>			
MINIMUM PROFICIENCY TARGET LEVELS				
<p>Job Skill Level 3: Intermediate GS 10-12</p>	<p>Job Skill Level 4: Advanced GS 12-14</p>	<p>Job Skill Level 4/5: Supervisor GS 13-14</p>	<p>Job Skill Level 5: Management GS 14-15</p>	
<p><b>2</b></p>	<p><b>3</b></p>	<p><b>4</b></p>	<p><b>5</b></p>	
BEHAVIORAL INDICATORS				
<p><b>Intermediate</b></p>	<ul style="list-style-type: none"> <li>• Performs review of an organization’s missions and determines capabilities, resilience, and criticality of functions.</li> <li>• Has an understanding of the installations’ and tenant unit mission and applies knowledge of these missions with assistance and guidance/supervision</li> <li>• Supports Mission Analysis and Mission Assurance Assessment (MAA) process and report development</li> <li>• Supports the review, update, and development of MA policy and procedures</li> </ul>			
<p><b>Advanced</b></p>	<ul style="list-style-type: none"> <li>• Assists leadership in determining criticality and resource requirements for critical missions</li> <li>• Provides guidance and oversight of MARPAs</li> <li>• Conducts Mission Analysis and MAA, reporting on vulnerabilities and risk mitigation activities</li> <li>• Reviews, updates, and develops MA policy, guidelines, data collection, reports, processes and procedures</li> </ul>			
<p><b>Supervisor</b></p>	<ul style="list-style-type: none"> <li>• Directs MAA Team (MAAT) according to prioritized schedule</li> <li>• Directs the review of policies, guidelines, data documents, reports, processes, and procedures</li> <li>• Manages or supervises multiple personnel in a proficient manner; consistently displays comprehensive and thorough knowledge of MA</li> <li>• Adapts to installation-specific requirements and can respond to a multitude of scenarios (e.g., EOC operations)</li> </ul>			
<p><b>Management</b></p>	<ul style="list-style-type: none"> <li>• Supports the Installation Commander, Fleet Marine Force Commanders and Higher Headquarters’ leadership (i.e., Deputy Commandants) with MA and integrated protection functions</li> <li>• Supports development of new policies and revises existing policies/procedures as necessary</li> <li>• Analyzes MAA trends and establishes critical mission risks based on MAAT reporting</li> <li>• Directs management of MARPAs</li> </ul>			

COMPETENCY	DEFINITION
<p><b>2. Critical Infrastructure Protection (CIP)</b></p>	<p>Critical infrastructure protection is a key pillar of the protection framework which supports and ensures successful execution of Marine Corps missions. Critical Asset Identification Process (CAIP) is used to identify and validate assets and infrastructures critical to the execution of Department of Navy (DON) and Marine Corps missions, tasks, core functions, and capabilities.</p>
<p><b>MINIMUM PROFICIENCY TARGET LEVELS</b></p>	

Job Skill Level 3: Intermediate GS 10-12	Job Skill Level 4: Advanced GS 12-14	Job Skill Level 4/5: Supervisor GS B13-14	Job Skill Level 5: Management GS 14-15
2	3	4	5
<b>BEHAVIORAL INDICATORS</b>			
<b>Intermediate</b>	<ul style="list-style-type: none"> <li>• Supports the development of Command Priority Intelligence Requirements (PIRs) and Critical Information Requirements (CIRs) specific to critical assets and infrastructures.</li> <li>• Reports Tier 1 and 2 mission critical asset non-availability, destruction, or degradation to Higher Headquarters (HHQ) when a change in status occurs</li> <li>• Understands and conducts the fundamentals of investigative procedures (e.g., basic crime scene investigation and protection) under supervision/guidance</li> <li>• Inputs CIP data, baseline elements of information (BEI), and all MAA reports into Marine Corps Critical Asset Management System (MC-CAMS)</li> </ul>		
<b>Advanced</b>	<ul style="list-style-type: none"> <li>• Shares Marine Corps authoritative CIP information with other DoD Components, including information on decisions made to acknowledge or manage risk to critical assets and infrastructures</li> <li>• Applies knowledge of critical infrastructure program for the execution of critical infrastructure protection and manages MC-CAMS at the organizational level</li> <li>• Supports the identification and submission of Marine Corps CIP requirements through the annual Planning, Programming, Budgeting, and Execution (PPBE) process</li> <li>• Develop processes to define, identify, document, and address risk to critical assets, infrastructures, Critical Program Information (CPI), and Defense Critical Assets owned or supported by the Marine Corps</li> <li>• Develops training packages for CAIP, Risk Management, and MC-CAMS</li> </ul>		
<b>Supervisor</b>	<ul style="list-style-type: none"> <li>• Oversees, manages, and directs the identification, validation, prioritization, and assessment of assets and infrastructures critical to the execution of Marine Corps missions, capabilities, core functions, and tasks. Plans and directs advanced violation detection activities (e.g., compliance checks, field interviews, preserving evidence, permit validation, surveillance)</li> <li>• Develops and maintains Marine Corps CIP program review standards and benchmarks to identify, monitor, and track execution of DoD, DON, and Marine Corps CIP requirements, goals, and objectives Approves the identification and submission of Marine Corps CIP requirements through the annual Planning, Programming, Budgeting, and Execution (PPBE) process</li> <li>• Reviews the quality and completeness of MC-CAMS BEI data, and identify gaps and trends that need to be addressed service-wide.</li> </ul>		
<b>Management</b>	<ul style="list-style-type: none"> <li>• Reviews and implements Memorandums of Understanding (MOU) with other law enforcement agencies</li> <li>• Ensures Marine Corps CIP program activities are synchronized with and align to MA risk management requirements</li> <li>• Serves as Chair of the organizations' Critical Infrastructure Protection Working Group (CIPWG)</li> </ul>		

	<ul style="list-style-type: none"> <li>• Manages the development and execution of MA and CIP support contracts</li> </ul>
--	---

COMPETENCY	DEFINITION
<b>3. Mission Assurance Risk Management</b>	MA risk management is the methodology used to assess and identify risk to critical assets and infrastructure. MA uses a risk-based framework to create synergies in implementing a standardized process for managing risk to the Fleet Marine Force and Supporting Establishment in the execution of their assigned missions, core functions, and related capabilities.
<b>MINIMUM PROFICIENCY TARGET LEVELS</b>	

Job Skill Level 3: Intermediate GS 10-12	Job Skill Level 4: Advanced GS 12-14	Job Skill Level 4/5: Supervisor GS 13-14	Job Skill Level 5: Management GS 14- 15
2	3	4	5
<b>BEHAVIORAL INDICATORS</b>			
<b>Intermediate</b>	<ul style="list-style-type: none"> <li>• Knowledge of the MA risk management methodology and assessments</li> <li>• Identifies criticality, threats/hazards, and vulnerabilities to assets and critical infrastructure</li> <li>• Prepares risk mitigation packages and mitigation action plans</li> </ul>		
<b>Advanced</b>	<ul style="list-style-type: none"> <li>• Applies the principles of risk management to the mission assurance construct</li> <li>• Conducts an organizational level risk assessment that includes criticality, threat/hazard, and vulnerability assessments</li> <li>• Conduct the All Hazard Threat Assessment (AHTA) and build the AHTA report.</li> <li>• Completes plans of actions and milestones for risk mitigation packages and mitigation action plans</li> </ul>		
<b>Supervisor</b>	<ul style="list-style-type: none"> <li>• Conducts senior level reviews and approvals of submitted risk mitigation packages and AHTAs</li> <li>• Ensures subordinate level personnel are following the MA risk management process</li> <li>• Utilizes the results of the risk assessment to identify and prioritize risk to missions and supporting critical assets and infrastructures.</li> </ul>		
<b>Management</b>	<ul style="list-style-type: none"> <li>• Ensures that all senior level reviews and approvals are submitted in timely manner</li> <li>• Develops policies and procedures for MA risk management; criticality, threat/hazard, and vulnerability assessments</li> <li>• Receives program reviews and provides guidance to action officers and staff</li> </ul>		

<b>COMPETENCY</b>	<b>DEFINITION</b>
<b>4. Protection Program Management</b>	Protection is a multi-dimensional grouping of functional areas applicable to the Fleet Marine Forces and Supporting Establishment. Protection serves as an enabler of the Service Campaign Plan and Operating Concepts and is essential for maximizing unity of effort, minimizing inefficiencies and enhancing service-wide management of prioritized risk to personnel, facilities, assets, infrastructure and information.

<b>MINIMUM PROFICIENCY TARGET LEVELS</b>			
<b>Job Skill Level 3: Intermediate GS 10-12</b>	<b>Job Skill Level 4: Advanced GS 12-14</b>	<b>Job Skill Level 4/5: Supervisor GS 13-14</b>	<b>Job Skill Level 5: Management GS 14-15</b>
<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>BEHAVIORAL INDICATORS</b>			
<b>Intermediate</b>	<ul style="list-style-type: none"> <li>• Is familiar with relationship between all of the Protection Programs</li> <li>• Supports the development of Protection Program plans of actions and milestones</li> <li>• Builds program policies and procedures with the aid of subject matter experts</li> </ul>		
<b>Advanced</b>	<ul style="list-style-type: none"> <li>• Advises and instructs others on the integration of Protection Programs</li> <li>• Understands and applies program management principles to the portfolio of Protection Programs</li> <li>• Conducts programs according to the industry standard project management principles</li> </ul>		
<b>Supervisor</b>	<ul style="list-style-type: none"> <li>• Ensures that integration of Protection Programs includes all aspects of the protection portfolio</li> <li>• Ensures the programs are executed according to project management principles and that in process reviews are executed as directed</li> <li>• Oversees the execution of Protection Programs by subordinates and contractor support personnel</li> <li>• Supports and directs actions of the Protection Organizational Advisory Group (OAG)</li> </ul>		
<b>Management</b>	<ul style="list-style-type: none"> <li>• Formulates, develops, and reviews Protection Program policies and procedures</li> <li>• Conveys and maintains Protection Program portfolio standards throughout the organization by directing related information sharing, training, and education</li> <li>• Serves as the Chair of various Protection Program working groups (i.e., Mission Assurance Working Group (MAWG), Antiterrorism Working Group, Senior Steering Group (SSG))</li> </ul>		

## Appendix B. Acronyms Defined

<b>Acronym</b>	<b>Definition</b>
AHTA	All Hazards Threat Assessment
BEI	Baseline Elements of Information

CAIP	Critical Asset Identification Process
CIP	Critical Infrastructure Protection
CIPWG	Critical Infrastructure Protection Working Group
CIR	Critical Information Requirement
COOP	Continuity of Operations
DCA	Defense Critical Asset
FMF	Fleet Marine Force
HHQ	Higher Headquarters
MA	Mission Assurance
MAA	Mission Assurance Assessment
MAAT	Mission Assurance Assessment Team
MARPA	Mission Assurance Related Program Activity
MAWG	Mission Assurance Working Group
MC-CAMS	Marine Corps Critical Asset Management System
OAG	Organizational Advisory Group
PPBE	Planning, Programming, Budgeting, and Execution
PIR	Priority Intelligence Requirement
SICA	Supporting Infrastructure Critical Asset
SSG	Senior Steering Group
TCA	Task Critical Asset
USMC	United States Marine Corps