

Security and Emergency Services Community of Interest

0080-Physical Security Security Administration

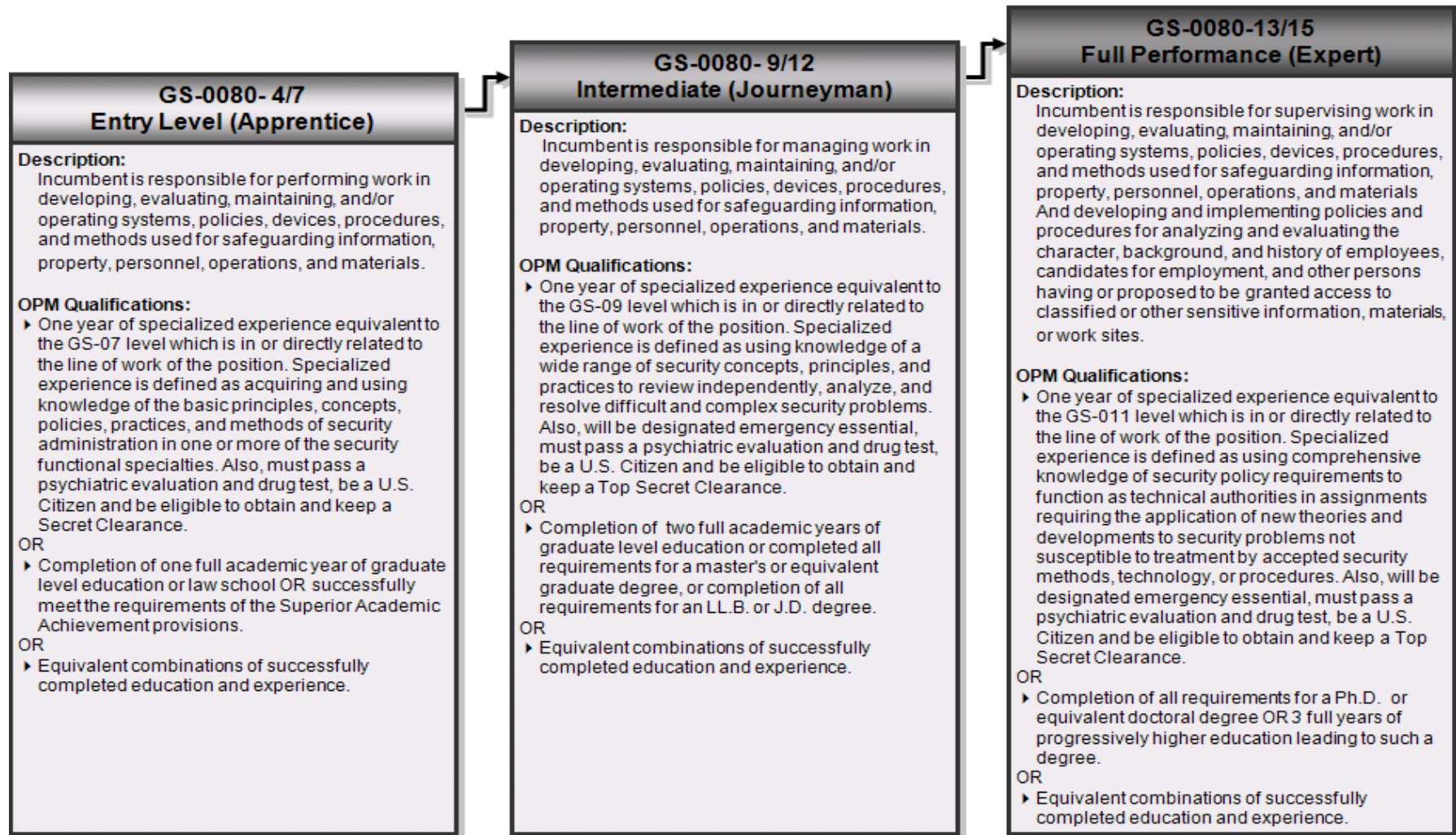
Career Road Map

Prepared by: Booz | Allen | Hamilton



“Support Our Marines Be Part Of The Team”

Career progression within the 0080-Physical Security Occupational Series is marked by advancing levels of expertise in matters of Security Administration



Proficiency and Skill Band Definitions for 0080-Physical Security

- ▶ The **Proficiency Rating Scale** below details the proficiency ratings and their corresponding definitions. Proficiency levels describe the levels of a 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.

PROFICIENCY RATING	PROFICIENCY
0	N/A - Non Applicable/No Knowledge Necessary
1	No Proficiency - Conceptual Knowledge Only/No Experience
2	Low Proficiency - Able to Apply with Help
3	Moderate Proficiency - Able to Apply Autonomously
4	High Proficiency - Proficient/Able to Help Others
5	Very High Proficiency - Expert Knowledge

- ▶ The Communities of Interest have outlined a career progress structure that more accurately reflects the change in your abilities and responsibilities over time. That structure is called the **Skill Level Structure**. It is associated with each Occupational Series and follows you from the time you are an entry-level employee until you reach management levels. Career progress in the USMC has traditionally been based on the Federal Government pay schedule system and the ranges within the pay schedule system are associated with the Skill Levels.

JOB SKILL LEVEL	SKILL BAND DEFINITION	JOB SKILL LEVEL PAY PLAN	BEGINNING GRADE	TARGET GRADE
1	Apprentice	GS	4	7
2	Journeyman	GS	9	12
3	Expert	GS	13	15

- ▶ Behavioral Indicators: It is important to define how the competencies are manifested at different proficiency levels. In other words, what behaviors do incumbents in the Occupational Series demonstrate that indicate various levels of proficiency in each competency area. These demonstrations are referred to as behavioral indicators, and provide an objective description of the behavior that you might view in an individual that provides evidence that they either have or do not have the competency of interest. These are **examples of what behaviors could look like** and are not inclusive of all behaviors that demonstrate each level of performance for the competency. Rather, this is a tool to help guide evaluations of employee performance and should **not** be used as a checklist for employees' behaviors.



Desired Certifications, Academic Credentials and Training for 0080-Physical Security

Level 1	Level 2	Level 3
Desired Certifications		
Army/FLETC/ASIS Physical Security Certification	Army/FLETC/ASIS Physical Security Certification	Army/FLETC/ASIS Physical Security Certification
Electronic Systems Administrator Certification	Naval Security Manager's Certification	Naval Security Manager's Certification
National Crime Prevention Institute Crime Prevention Specialist Certification	National Crime Prevention Institute Crime Prevention Specialist Certification	National Crime Prevention Institute Crime Prevention Specialist Certification
	DoD Lock Specialist Certification	DoD Lock Specialist Certification
	Basic Antiterrorism II Certification	Basic Antiterrorism II Certification
	US Army Corps of Engineers-Electronic Security Systems Design Certification	US Army Corps of Engineers-Electronic Security Systems Design Certification
Desired Academic Credentials		
High School Graduate	Any BS/BA Degree	Any BS/BA Degree
Any AA/BS/BA Degree		Any MS/MA Degree
Desired Training		
	DoD Security Engineering Planning and Standards	DoD Security Engineering Planning and Standards

**The courses found on this page and throughout this roadmap are recommended courses and may not be inclusive of all training available.*



“Support Our Marines Be Part Of The Team”

Behavioral Indicators

Physical Security Program Management

DEFINITION

Oversees and supports programs and implementation of protective measures that ensure mission accomplishment and enhance the security of installations/facilities and its contents in compliance with Department of Defense (DoD) and Marine Corps regulations, directives, and policies. Provides subject matter expertise to installations and commanders.

Entry	Intermediate	Full Performance
<ul style="list-style-type: none"> - Has a knowledge and understanding of the components and factors comprising the applicable physical security functional area (e.g., CBRNE, CIP, Industrial Security, Antiterrorism, Crime Prevention, Flight Lines / Restricted Area, Arms, Ammunition, and Explosives (AA&E), Classified Information Storage Spaces, and Classified Materials Security) - Has a knowledge of security requirements in the applicable physical security functional area (e.g., how to set physical security parameters) - Conducts inspections for compliance with physical security requirements - Reads and interprets blueprints and applies requirements 	<ul style="list-style-type: none"> - Integrates and coordinates physical security activities with those internal and external to the organization - Analyzes threats in the applicable physical security functional area - Implements and applies systems to mitigate threats to physical security - Interprets physical security requirements as they impact existing or planned work/activities - Reviews compliance inspections for accuracy and completeness before submission to command - Ensures organizational compliance with physical security requirements - Determines whether infrastructure will support certain technologies - Ensures security requirements are in compliance with applicable orders and directives - Reviews blueprints and applies requirements - Develops and provides mitigating requirements in case of non-compliance - Assists in submission of exception/waiver requests 	<ul style="list-style-type: none"> - Provides Marine Corps leadership with requisite knowledge to make informed security decisions - Writes physical security plans, policies, and procedures - Mentors and educates less experienced staff on compliance inspection criteria, protocols, and procedures - Builds awareness of emerging physical security technologies and requirements - Formulates strategic plans and the future vision of the physical security program - Ensures compliance of large-scale projects with applicable orders and directives - Establishes and submits budgets - Develops and provides mitigating requirements in case of non-compliance - Assists in submission of exception/waiver requests



“Support Our Marines Be Part Of The Team”

Competency-Based Training Opportunities

Physical Security Program Management

Skill Level	Proficiency		DEFINITION
	Min	Max	
1	1	2	Oversees and supports programs and implementation of protective measures that ensure mission accomplishment and enhance the security of installations/facilities and its contents in compliance with Department of Defense (DoD) and Marine Corps regulations, directives, and policies. Provides subject matter expertise to installations and commanders.
2	3	4	
3	4	5	

Course	Skill Level	Institution
Antiterrorism Force Protection (ATFP) Workshop	1,2,3	NAVAC ESC
Basic CPTED (Crime Prevention Through Environmental Design)	1,2,3	NCPI
Basic Crime Prevention Certification Seminar	1,2,3	ACPI
Basic Crime Prevention Through Environmental Design (CPTED) Seminar	1,2,3	ACPI
Comprehensive Security Specialist	1,2,3	LSI
Comprehensive Security Specialist	2,3	LSI
DCID 6/9 Physical Security Seminar	2,3	DSSA
Introduction to Physical Security Course	1,2	DSSA
Lighting Technology	1,2,3	Lighting Education Online
Lighting Terminology	1,2,3	Lighting Education Online
Physical Security Professional (PSP) Development Course	2,3	ASIS International
Physical Security Training Program (PSTP)	2,3	FLETC
Residential Lighting	1,2,3	Lighting Education Online



“Support Our Marines Be Part Of The Team”

Behavioral Indicators

Electronic Security Systems Management

DEFINITION

Ensures effective operation and maintenance of electronic security systems. Identifies electronic security requirements, oversees system installation, conducts compliance inspections, and proposes electronic security solutions. Safeguards installation assets through the use of electronic security systems. Demonstrates knowledge of emerging technology areas (e.g., biometrics, surveillance, access control, CCTV, intrusion detection, radar, encryption, CBRNE detection, etc.).

Entry	Intermediate	Full Performance
<ul style="list-style-type: none"> - Has a knowledge of security requirements in applicable electronic security functional areas (e.g., how to set physical security parameters) - Conducts inspections for compliance with electronic security requirements with close supervision - Records and submits electronic security system issues for repair/resolution - Operates basic security systems - Awareness of emerging security technology areas (e.g., attending conferences/symposiums) - Conducts Media research to understand state of the market, existing technologies - Understands security requirements as it relates to technologies - Understands minimum protection requirements for ESS - Tests operational status of ESS 	<ul style="list-style-type: none"> - Conducts inspections for compliance with electronic security requirements - Submits requests for installation of new and upgrades to existing electronic security systems - Performs diagnostics, conducts basic maintenance on, and submits requests for repair/resolution of electronic security system - Identifies electronic security requirements - Trains electronic security system operators on system problem identification and response - Prepares and presents emerging technologies at conferences/symposiums - Identifies deficiencies in existing technologies - Evaluates effectiveness of existing technologies and upgrades - Understands systems integration - Tests operational status of ESS - Prepares and submits budget - Evaluates system integration 	<ul style="list-style-type: none"> - Coordinates/manages submission of requests for installation of new and upgrades to existing electronic security systems - Validates electronic security requirements - Identifies and evaluates electronic security solutions to determine effectiveness and feasibility - Proposes new electronic security technologies for consideration by Headquarters - Performs electronic security system issue trend analysis and problem resolution - Organizes and speaks at emerging technologies conferences/symposiums - Provides recommendations for the evaluation and applicability of new technologies - Provides input and guidance to the development of new technologies - Identifies threats vulnerabilities of new technology - Integrates security technology capabilities in security program - Reviews, approves, and forwards budget submission



“Support Our Marines Be Part Of The Team”

Competency-Based Training Opportunities

Electronic Security Systems Management

Skill Level	Proficiency		DEFINITION
	Min	Max	
1	1	2	Ensures effective operation and maintenance of electronic security systems. Identifies electronic security requirements, oversees system installation, conducts compliance inspections, and proposes electronic security solutions. Safeguards installation assets through the use of electronic security systems. Demonstrates knowledge of emerging technology areas (e.g., biometrics, surveillance, access control, CCTV, intrusion detection, radar, encryption, CBRNE detection, etc.).
2	3	4	
3	4	5	

Course	Skill Level	Institution
DCID 6/9 Physical Security Seminar	2,3	DSSA
Electronic Security Systems Administrators Course	1,2,3	SPAWAR
Electronic Security Systems Design Course	1,2,3	USACE PDC



“Support Our Marines Be Part Of The Team”

Behavioral Indicators

Access Control

DEFINITION

Controls access and prevents unauthorized access to personnel, equipment, material, documents, and safeguards against espionage, sabotage, acts of terrorism, damage, and theft.

Entry	Intermediate	Full Performance
<ul style="list-style-type: none"> - Understands the concepts related to denial of access to restricted facilities - Understands and operates barrier systems to control vehicular and personnel movement - Determines whether the physical safeguarding requirements for restricted areas are met - Understands and implements signage requirements for restricted areas - Applies policy requirements to facilities/areas - Inspects equipment - Identifies various options for equipment 	<ul style="list-style-type: none"> - Determines the physical safeguarding requirements for restricted areas - Designs and maintains security accountability, control methods, and tools - Responsible for the inspection and oversight of access control procedures - Implements and maintains specialized access control programs for restricted areas (e.g., classified material storage, COMSEC, Flight Lines) - Assists in the conduct of preliminary inquiries into physical and electronic security violations - Trains personnel in systems operations - Identifies various options for equipment - Develops barrier plan - Reviews new technology 	<ul style="list-style-type: none"> - Makes recommendations to Commander regarding issues of access control regarding security posture - Ensures that appropriate restriction level standards are maintained - Implements new physical and electronic security policies - Mentors and educates less experienced staff or external personnel on security regulations, directives, and policies - Recommends courses of action for remediation, mitigation, or correction of security violations - Approves barrier plan - Evaluates and approves systems integration



“Support Our Marines Be Part Of The Team”

Competency-Based Training Opportunitites

Access Control			
Skill Level	Proficiency		DEFINITION
	Min	Max	
1	1	2	Controls access and prevents unauthorized access to personnel, equipment, material, documents, and safeguards against espionage, sabotage, acts of terrorism, damage, and theft.
2	3	4	
3	4	5	
Course		Skill Level	Institution
Access Control Point Training		2,3	USACE PDC
Access Control Technician (ACT)		2,3	LSI
Comprehensive Security Specialist		1,2,3	LSI
Comprehensive Security Specialist		2,3	LSI
DCID 6/9 Physical Security Seminar		2,3	DSSA
Lock and Key Systems Course		1,2,3	DSSA
Physical Security Measures Course		1,2	DSSA
SDDCTEA		1,2,3	SDDCTEA



“Support Our Marines Be Part Of The Team”

Behavioral Indicators

Security Awareness, Education, & Training

DEFINITION

Provides for the development, execution, and evaluation of educational programs (such as Welcome Aboard Briefs) to ensure security awareness, education, and training.

Entry	Intermediate	Full Performance
<ul style="list-style-type: none"> - Knowledge of principles, practices, policies, and techniques of training, education, and employee development - Possesses a broad understanding of overall security programs and policies - Comprehends concepts and intended purpose of security requirements (e.g., accountability and control standards, threat conditions) - Communicates security requirements with minimal guidance - Understands organizational mission requirements and the relationship with security - Prepares training materials (e.g., presentations, guides) - Prepares media presentations for dissemination 	<ul style="list-style-type: none"> - Delivers training and education on security requirements relevant to the mission of the organization - Identifies deficiencies in security training, education, and awareness (e.g., violation evaluation, surveys, trend analysis) - Designs training materials (e.g., presentations, guides) in alignment with performance and learning objectives - Approves media presentations 	<ul style="list-style-type: none"> - Develops security requirements training, education, and outreach programs - Evaluates security training, education, and awareness deficiencies and develops programs/initiatives to address gaps - Educates leadership on the value added of security training, education, and awareness programs - Identifies training, education, and awareness resources - Advocates senior leadership buy-in to security awareness, education, and training programs - Uses innovative technologies to facilitate the development and delivery of training, education, and awareness programs



“Support Our Marines Be Part Of The Team”

Competency-Based Training Opportunities

Security Awareness, Education, & Training

Skill Level	Proficiency		DEFINITION	
	Min	Max		
1	1	2	Provides for the development, execution, and evaluation of educational programs (such as Welcome Aboard Briefs) to ensure security awareness, education, and training.	
2	3	4		
3	4	5		
Course			Skill Level	Institution
Conventional Physical Security Course			1,2,3	USAMP FPTD
Crime Prevention and Introduction to Physical Security			1,2	NCPI
DoD Security Engineering Planning and Standards			2,3	USACE PDC
Security Engineering			2,3	USACE PDC



“Support Our Marines Be Part Of The Team”

Behavioral Indicators

Acquisition Management

DEFINITION

Uses Knowledge of acquisition management functions, practices, and policies, and an understanding of how these functions contribute to the accomplishment of the organization's mission.

Entry	Intermediate	Full Performance
<ul style="list-style-type: none"> - Knowledge of Defense Federal Acquisition Regulations (DFAR) and general acquisition and contracting principles - Awareness of the acquisition process and the relationship between industry and government - Understands basic acquisition rules (e.g., obligation of government funds) - Understands MARCORSSYSCOM's authority and role in the acquisition/contracting process - Understands sources of funding (e.g., MILCON, PSUP funds, etc.) and how they are aligned with various project types 	<ul style="list-style-type: none"> - Understands security restrictions and prohibitions as it relates to acquisitions, contracts, and the performance of work - Evaluates and provides feedback on physical security-related outputs of contracts as part of a larger program - Understands sources of funding (e.g., MILCON, PSUP funds, etc.) and how they are aligned with various project types 	<ul style="list-style-type: none"> - Defines operational requirements and identifies the need for acquisition and contracting activities to meet requirements - Develops technical requirements for Statements of Work (SOWs) in collaboration with contracting and procurement personnel - Manages contractual agreements to ensure quality standards are met and kept - Manages acquisitions and contracts for programs in support of mission objectives - Provides physical security input to source selection board as part of a larger program



“Support Our Marines Be Part Of The Team”

Competency-Based Training Opportunities

Acquisition Management			
Skill Level	Proficiency		DEFINITION
	Min	Max	
1	1	2	Uses Knowledge of acquisition management functions, practices, and policies, and an understanding of how these functions contribute to the accomplishment of the organization's mission.
2	3	4	
3	4	5	
Course		Skill Level	Institution
ACQ 101 Fundamentals of Systems Acquisition Management		1,2	DAU
ACQ 201A Intermediate Systems Acquisition, Part A		2,3	DAU
ACQ 201B Intermediate Systems Acquisition, Part B		2,3	DAU
ACQ 451 Integrated Acquisition for Decision Makers		3	DAU
ACQ 452 Forging Stakeholder Relationships		3	DAU



“Support Our Marines Be Part Of The Team”

Behavioral Indicators

Risk Management

DEFINITION

Identifies critical assets, threats and vulnerabilities, and mitigation strategies to arrive at an acceptable level of risk throughout a physical security program along with recording, maintaining, and reporting various risk management activities.

Entry	Intermediate	Full Performance
<ul style="list-style-type: none"> - Understands risk management process, principles, concepts, and application - Participates and assists in the risk management process - Participates in the identification of critical assets 	<ul style="list-style-type: none"> - Applies risk management process, principles, and concepts - Participates in the analysis, evaluation, development, coordination, and dissemination of risk management methods and tools - Defines and analyzes risk management, assessment, and mitigation procedures in accordance with organizational goals 	<ul style="list-style-type: none"> - Develops and recommends risk management courses of action to senior leadership - Develops specific risk management policies and procedures; considers risk as a basis for every policy decision that is made - Participates in cross-functional risk management planning with other security disciplines (e.g., Information, Personnel)



“Support Our Marines Be Part Of The Team”

Competency-Based Training Opportunities

Risk Management			
Skill Level	Proficiency		DEFINITION
	Min	Max	
1	1	2	Identifies critical assets, threats and vulnerabilities, and mitigation strategies to arrive at an acceptable level of risk throughout a physical security program along with recording, maintaining, and reporting various risk management activities.
2	3	4	
3	4	5	
Course		Skill Level	Institution
GSA Certified Safe and Vault Technician with GSA Approved Inspector Option		2,3	MBA USA, INC.
Physical Security Measures Course		1,2	DSSA
Risk Management for DoD Security Programs Course		2,3	DSSA

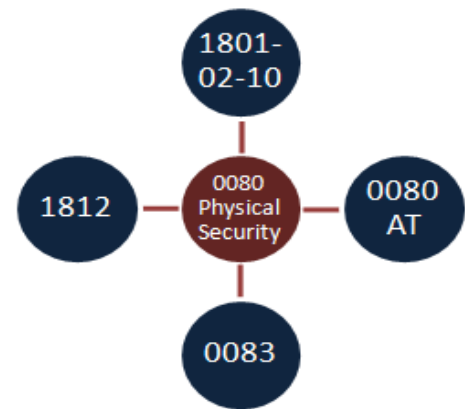


“Support Our Marines Be Part Of The Team”

Security Emergency Services Internal Community Career Path

0080 Physical Security			
1801-02-10 General Investigation	0080 AT	0083 Police	1812 Environmental Law Enforcement
<ul style="list-style-type: none"> •Competency Gaps: Non-Criminal Investigations; Evidence Recognition, Collection & Analysis •No Certification Gaps •GS5-8 is the recommended level to cross over 	<ul style="list-style-type: none"> •Competency Gaps: AT Program Review •Certification Gaps: DSTC Designated Certification; FEMA Professional Development Series Certification; Level II AT •GS9-11 is the recommended level to cross over 	<ul style="list-style-type: none"> •Competency Gaps: Basic Investigation & Reporting; Traffic Enforcement •No Certification Gaps •GS3-6 is the recommended level to cross over 	<ul style="list-style-type: none"> •Competency Gaps: Criminal Investigation; Fish & Wildlife Laws •No Certification Gaps •GS9 is the recommended level to cross over

This graphic shows the 0080 Physical Security series other series that they can cross over into and be competitive in the hiring process. A **Competency Gap** is the difference between the current competency level of employees and the required competency level. A **Certification Gap** is the difference between the current certification levels of employees and the required certification levels.



"Support Our Marines Be Part Of The Team"

Acronyms Defined

Acronym	Acronym Defined
ACPI	American Crime Prevention Institute
DAU	Defense Acquisition University
DSSA	Defense Security Service Academy
FLETC	Federal Law Enforcement Training Center
LSI	Laboratory for Scientific Interrogation
MBA USA, INC.	MBA USA, INC.
NAVAC ESC	Naval Facilities Engineering Command Engineering Service Center (NAVAC ESC)
NCPI	National Crime Prevention Institute
SDDCTEA	Surface Deployment and Distribution Command Transportation Engineering Agency (SDDCTEA)
SPAWAR	Space and Naval Warfare Systems Command
USACE PDC	United States Army Corps of Engineers Protective Design Center (USACE PDC)
USAMP FPTD	United States Army Military Police School, Force Protection Training Division

**For additional courses supporting the following behavioral competencies: Communication, Leadership, Self Management and Planning, Decision Making, Problem Solving, Teamwork, and Health Safety please refer to the Civilian leadership Development (CLD) Course Catalog. This catalog can be found on this website:*

https://www.manpower.usmc.mil/pls/portal/docs/PAGE/M_RA_HOME/MP/MPC/CWM/TRAININGRESOURCES/CIVILIAN%20LEADERSHIP%20COURSE%20CATALOG/MP_MPC_TR_C_LCC_REF/FULL%20COURSE%20CATALOG.PDF



“Support Our Marines Be Part Of The Team”