



# Overview of Electronic Security Systems

Presented to  
NAVAFAC FAR EAST

John Lynch, P.E. and Julie Heup, P.E.  
Planning, Design and Construction Criteria (PDCC)  
Engineering Criteria and Programs

October 2024

## NAVADMIN 193/22 Interim Guidance for the Life Cycle Management of Shore Electronic Security Systems

- NAVADMIN 193/22 was issued by OPNAV N46 to change the way the Navy procures, installs and maintains Electronic Security Systems (ESS).Lead Agency: Navy
- BLUF: NAVFAC will be going back to providing the infrastructure and NIWC LANT will provide the ESS equipment as outlined below.

### REFERENCES

<b>REF A</b> IS DOD S-5210.41-M, Nuclear Weapon Security Manual.	<b>REF H</b> IS OPNAVINST 11010.20H, Naval Facility Projects Manual.
<b>REF B</b> IS OPNAVINST 5530.14E, Navy Physical Security And Law Enforcement Program.	<b>REF I</b> IS SECNAVINST 5510.36B, Department Of The Navy Information Security Program.
<b>REF C</b> IS OPNAVINST 5530.13D, The Conventional Arms, Ammunition And Explosives Physical Security Policy Manual.	<b>REF J</b> IS DODM 5200.01 Volume 3, DOD Information Security Program: Protection Of Classified Information.
<b>REF D</b> IS CNICINST 5530.14A, Ashore Protection Program.	<b>REF K</b> IS UFC 4-010-06, Cybersecurity Of Facility-Related Control Systems.
<b>REF E</b> IS DODINST 8510.01, Risk Management Framework For DOD Systems.	<b>REF L</b> IS UFC 4-021-02, Electronic Security Systems.
<b>REF F</b> IS DODM O-5205.07, Volume 3 Special Access Program (Sap) Security Manual: Physical Security.	<b>REF M</b> IS SECNAVINST 5400.15D Research And Development, Acquisition, Associated Lifecycle Management, And Sustainment Responsibilities And Accountability
<b>REF G</b> IS The Intelligence Community Standard (ICS) 705-1, Physical And Technical Security Standards For Sensitive Compartmented Information Facilities.	<b>REF N</b> IS OPNAVINST 5210.16A, Security Of Nuclear Reactors And Special Nuclear Material

NAVFAC

## NAVADMIN 193/22

### Interim Guidance for the Life Cycle Management of Shore Electronic Security Systems


- **BACKGROUND.** Installation commanding officers have an inherent responsibility to provide protection for their installations.
  - This is accomplished through the employment of a **defense in depth (aka security in depth)** approach, to **include the use of ESS.**
  - A lack of policy encouraging standardization of ESS employment has resulted in **inconsistent responsibilities and procurement practices;** fostering a wide variety of requirements, installation and maintenance/sustainment practices.
  - Deputy Chief of Naval Operations, Fleet Readiness and Logistics (OPNAV N4) intends to **streamline and standardize** the procurement, installation, sustainment, and training for ESS across the shore domain.
  - **Overall goals are to reduce waste in resourcing across the Service, improve existing and future system configurations and cyber fitness, and reduce the need for various exchanges to engage with vendors for procurement and sustainment of various systems.**

NAVFAC

## NAVADMIN 193/22

### Interim Guidance for the Life Cycle Management of Shore Electronic Security Systems

- **POLICY:** Under the authority of OPNAV N4, and as a component of the Navy Physical Security Program, ESS is understood to include:
  - Integrated (or stand-alone) electronic systems that encompass interior and exterior intrusion detection systems (IDS)
  - Closed circuit television or video surveillance systems (for assessment of alarm conditions)
  - Access control systems; Alarm reporting systems for monitoring, control, and/or display; duress devices, and other associated components such as **data transmission media (DTM).**
  - For the purposes of this policy, **DTM refers only to communications and network components categorized as personal property per OPNAVINST 11010.20J Navy Facilities Projects.**
  - **ESS for designated restricted areas will be procured and deployed in accordance with respective security policies. This includes security requirements associated with installation perimeter access control and restricted areas as defined by policy.**
  - ESS for restricted areas will be centrally monitored at a location from which law enforcement/security response can be dispatched. Central (regional) and local monitoring stations will be manned by certified operators.




## NAVADMIN 193/22

### Interim Guidance for the Life Cycle Management of Shore Electronic Security Systems

- **POLICY:** Under the authority of OPNAV N4, and as a component of the Navy Physical Security Program, ESS is understood to include (continued):
  - All ESS employment will be executed by a **single warfare center** for execution of ESS projects in support of Navy requirements.
    - **NIWCLANT: Naval Information Warfare Center (NIWC) Atlantic** provides systems engineering and acquisition to deliver information warfare capabilities to the naval, joint and national warfighter through the acquisition, development, integration, production, test, deployment and sustainment of interoperable command, control, communications, computer, intelligence, surveillance and reconnaissance, cyber and information technology capabilities. (From website: <https://www.niwcatlantic.navy.mil/>)
  - The **Navy ESS technical manager** will provide support to all Navy tenants, **including Commander, Naval Facilities Engineering Systems Command (COMNAVFACENGSYSCOM)** for construction and special projects (i.e. military construction (MCON) and facilities sustainment, and restoration and modernization (SRM) funded projects). This technical support will extend to Navy tenants on other Service installations, and off installation areas as deemed appropriate by Director, Installations (OPNAV N4I) and Commander, Navy Installations Command (CNIC).

**NIWCLANT is ESS Technical Manager**



## NAVADMIN 193/22

### Interim Guidance for the Life Cycle Management of Shore Electronic Security Systems - Roles and Responsibilities

- **OPNAV N4I, will:**
  - 1) Update reference (b) (PS/LE) to ensure ESS requirements and definitions are clearly defined for designated restricted areas;
  - 2) Serve as the single Resource Sponsor for required Navy ESS;
  - 3) Develop and validate requirements for all Navy ESS submitted during the Program Objective Memorandum (POM) cycle;
  - 4) Identify resources associated with existing non-CNIC ESS requirements for realignment to OPNAV N4;
  - 5) Publish guidance annually with business rules for year of execution procurement and emergent needs.
  - 6) OPNAV N4I Director - Installations.
  - 7) OPNAVINST 5530.14E, Navy Physical Security And Law Enforcement Program – currently under revision.
  - 8) OPNAVINST 5450.352B Funding/Money - A resource sponsor represents a specific program and navigates through the dynamics and complexities of the Planning, Programming, Budgeting and Execution System (PPBES)/POM cycle.
  - 9) **Ensure ESS that was procured/installed/sustained by the supported command as personal equipment as defined by OPNAVINST 11010.20J.**

**NOTE: See NAVFACENGSYSCOM MCON/MCNR Review Board Consistency Review Board (CRB)/BPMS Guidelines for DD 1391 Development**

## NAVADMIN 193/22


### Interim Guidance for the Life Cycle Management of Shore Electronic Security Systems - Roles and Responsibilities

- **CNIC will:**
  - 1) Act as the **single Navy Program Office** for ESS deemed valid by OPNAV N4I. All Navy ESS Program funded systems will be owned by, and the responsibility of, the ESS Program;
  - 2) Serve as the **single budget submitting organization (BSO)** and **System Owner** for the Navy ESS Program;
  - 3) Update reference (d) (Ashore Protection) to ensure ESS requirements are defined for all Echelon 2 and subordinate Commands;
  - 4) Coordinate with **Naval Information Warfare Center Atlantic (NIWCLANT)** to validate current ESS footprint for applicable restricted areas on all installations;
  - 5) Develop an education campaign for region and installation personnel on Navy ESS programmatic and business cycle guidance;
  - 6) Provide a report annually no later than the 4th quarter of each fiscal year that includes a status of the program and emergent and planned requirements for POM planning;
  - 7) **As office of primary responsibility for Navy ESS Program, continue execution of other physical security equipment categorized as real property (automated vehicle barriers, waterside security defense systems, automated vehicle gates, automated pedestrian turnstiles) ensuring system integration with ESS where feasible;**

## NAVADMIN 193/22

### Interim Guidance for the Life Cycle Management of Shore Electronic Security Systems - Roles and Responsibilities

- **CNIC will: (CONTINUED)**
  - 8) Ensure **Navy ESS project management, execution and sustainment** is supported by and incorporated within the approved information management system; (AIM/REMEDY)
  - 9) **Maintain an inventory** of all required Navy ESS located on Navy installations;
  - 10) **Participate in and coordinate with applicable working groups** with the purpose of developing and standardizing processes supporting systems standardization, cybersecurity, development of best practices, integration, and life-cycle management (i.e. maintenance, sustainment, technology refreshment) for ESS;
  - 11) Ensure all installation and life cycle management of ESS adhere to the requirements set forth in references (e) and (k); (RMF and Cybersecurity)
  - 12) Coordinate with **Security Equipment Integration Working Group (SEIWG)** and participate in reoccurring events, to foster physical security equipment interoperability ensuring compliance with SEIWG (SEIWG National Information Exchange Model (NIEM) Information Exchange Package Documentation) and NIEM standards, per DOD I 8320.07;
  - 13) Establish and maintain a formal training program to support end user and technical support personnel system familiarization. **The training will encompass the approved ESS Family of Systems (FOS).**



## NAVADMIN 193/22


### Interim Guidance for the Life Cycle Management of Shore Electronic Security Systems - Roles and Responsibilities

- **CNIC IS:**
  - 1) CNIC N6S Public Safety Systems Program/NEEPO Electronic Security Systems
  - 2) Procured/Installed/Sustained through CNIC N6S
  - 3) OPNAV N4I will be the resource sponsor for the required ESS.
  - 4) Procure, install, and sustain.
  - 5) Provide funding requirements to OPNAV N4I
  - 6) CNICINST 5530.14A, Ashore Protection Program superseded by **CNIC M (Manual) 5530.1, Commander, Navy Installation Command Ashore Protection Program (2020).**
  - 7) **NIWCLANT – Technical Manager**
  - 8) **TRAINING** – Check with CNIC N6S website for Training Materials where there are presentations on business cycles and what is funded/not funded by CNIC N6S

**REGARDING ITEMS 1-13 on the previous slides, CNIC N6S SEEMS TO PRETTY MUCH HAVE THIS IN HAND WITH THEIR EXISTING EQUIPMENT RESPONSIBILITIES THROUGH AIM AND REMEDY (WEBSITE/PORTAL FOR PSE/ESS MANAGEMENT).**

**AS THE NAVY PROGRAM OFFICE (NOT THE RESOURCE OFFICE):**

- **CNIC N6S will then distribute to NIWCLANT the funds to provide the ESS based on the policy based requirements.**



## NAVADMIN 193/22

### Interim Guidance for the Life Cycle Management of Shore Electronic Security Systems - Roles and Responsibilities

- **Naval Information Warfare Systems Command (NAVWAR) will:**
  - 1) Support the Navy ESS Program ensuring compliance with engineering and cybersecurity standards;
  - 2) Provide technical expertise **in support** of CNIC shore ESS program management efforts.
- **NIWCLANT provides systems engineering and acquisition to deliver information warfare capabilities to the naval, joint and national warfighter through the acquisition, development, integration, production, test, deployment and sustainment of interoperable command, control, communications, computer, intelligence, surveillance and reconnaissance, cyber and information technology capabilities and will:**
  - 1) Serve as the **Technical Manager for Navy ESS, supporting N4I and CNIC** in Programming and Planning for shore ESS initiatives;
  - 2) **Execute requirements** on behalf of CNIC for the procurement, installation, training, and sustainment of ESS;
  - 3) Provide training for ESS to system operators, physical security specialists, and field service representatives. Additional billets may be added to participate in training, with approval from CNIC;
  - 4) Provide **COMNAVFACENGSYSCOM preliminary ESS layouts and one-line diagrams to include in the construction project solicitation documents**;
  - 5) Review construction project design submittals and provide comments to **COMNAVFACENGSYSCOM** on ESS layouts.

## NAVADMIN 193/22

### Interim Guidance for the Life Cycle Management of Shore Electronic Security Systems - Roles and Responsibilities

- COMNAVFACENGSSCOM (NAVAFAC) will:
  - 1) Serve as **Technical Authority** for facility engineering design and construction in accordance with reference (m).
  - 2) Ensure that construction **projects include necessary infrastructure (Real Property)** as defined by reference (h) (20J) to support the ESS when those systems are required;
  - 3) Coordinate ESS infrastructure layouts for construction projects with NIWCLANT; (See d(4) above in NIWCLANT.
  - 4) Ensure that ESS is **not acquired outside of the process** described above;
  - 5) Notify the CNIC ESS Program office of **all** requests for ESS.
  - 6) AS TECHNICAL AUTHORITY:
    - NAVFAC will no longer utilize the MILCON contractor to provide the ESS equipment.
    - The MILCON will only provide the infrastructure (empty conduit system) that supports ESS.
    - NAVFAC has not been informed on what happens when the supported command wants additional ESS above what is required for accreditation of the space.
    - Those and other details have not been worked out.
    - In those cases, the supported command should contact CNIC N6S for additional information.
    - **Currently, the additional ESS is funded by the requesting/supported command.**
  - 7) NAVFAC will provide empty conduit systems (infrastructure) to support the procurement and installation of ESS by NIWCLANT.

## NAVADMIN 193/22

### Interim Guidance for the Life Cycle Management of Shore Electronic Security Systems - Roles and Responsibilities

- Regional Commands, Installation Commanding Officers and Tenant Commands will:
  - 1) **Publish** this policy to all subordinate commands/activities.
  - 2) **Ensure that ESS is not procured outside of the requirements described above;**
  - 3) **Ensure that ESS requirements are identified early in project planning – DD 1391 Development;**
  - 4) Direct all requests for ESS to the POCs identified by the CNIC ESS Program office, via the information management system approved by OPNAV N4I;
  - 5) Enable the installation physical security department as the single point of contact at the installation level to support ESS requests;
  - 6) Designate in writing installation physical security personnel to act on behalf of Installation Commanding Officer and Installation SECO by participating in facilities planning discussions (MILCON, FSRM, etc.) ensuring physical security and ESS requirements are identified;
  - 7) **Ensure installation physical security personnel are identified as the initial POC for ESS project oversight, maintenance, and sustainment.**

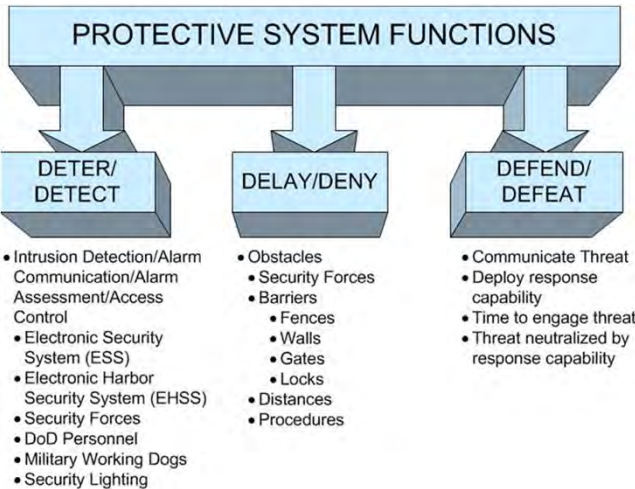


## Electronic Security System (ESS)

- The integrated electronic security system that encompasses interior and exterior Intrusion Detection Systems (IDS), Closed Circuit Television (CCTV) systems for assessment of alarm conditions, Automated Access Control Systems (ACS), Data Transmission Media (DTM), and alarm reporting systems for monitoring, control, and display. ESS equipment includes items such as sensors, cameras, card readers, processing control units (PCU), field panels, and workstations.
  - IDS: A system consisting of interior and exterior sensors, surveillance devices, and associated communication subsystems that collectively detect an intrusion of a specified site, facility, or perimeter and annunciate an alarm.
  - CCTV: The system interior and exterior cameras, monitors, archiving hardware, and associated communication subsystems that allow video archiving and assessment of alarm conditions via remote monitoring.
  - ACS: The system consisting of card readers, electronic locks, and the associated communication subsystem that ensures only authorized personnel are permitted ingress and egress into the protected area.

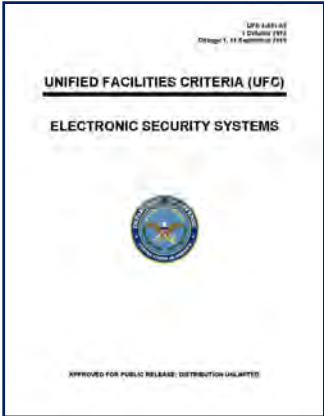
## Protective System Functions

- Comprised of three major sub-functions: Detect, Delay/Deny, and Defend/Defeat.



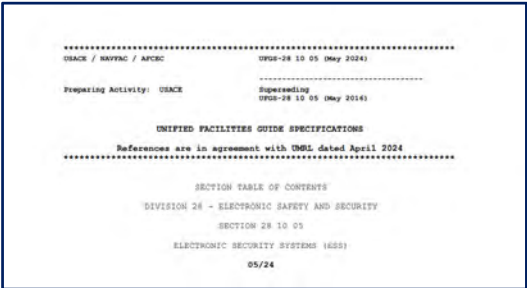
# UFC 4-021-02 Electronic Security Systems

- **Purpose:**
  - Provide effective and efficient criteria for designing Electronic Security Systems (ESS) in support of the Department of Defense (DoD) physical security program requirements.
- **Lead Agency: Navy**
  - Point of contact: John Lynch/Julie Heup/Rob Boller
- **Current Document Status:**
  - Originally Published 2006
  - Revision Published 1 October 2013
    - Unification
    - Format
    - Technology
    - Lessons learned
  - Change 1 published 11 September 2019
  - Complete Revision currently up to CP/ESEP for signature



## UFGS for ESS

- **UFGS 28 10 05 Electronic Security Systems (ESS)**
  - Published May 2024
- **UFGS 28 08 10 Electronic Security System Acceptance Testing**
  - Published August 2023





## Physical Security System

### Security professionals design systems by:

- **Combining protective measures and operational procedures into an integrated system that works within a installation's, facility's, and user's constraints**
  - Components should complement each other and correct for vulnerabilities.
  - Contain supporting elements coordinated to prevent gaps or overlaps in responsibilities and performance.

## The Problem

# Where Do We Start?



## Assets

- **Determining the assets is the first step in establishing any protective system**



## What Generates the Requirement for ESS?

- **The asset being protected and the associated regulatory guidance or policy generates the requirement.**
  - Arms, Ammunitions, and Explosives (AA&E)
  - Classified Materials (Secret and above)
  - Classified Communications System
    - SIPRNet
    - JWICS
  - Sensitive Compartmented Information (SCI)
  - Special Access Program Information (SAPI)
  - Installation Access Control Facilities (ECF/ACP)

## POLICY

- **AA&E:** OPNAV INSTRUCTION 5530.13C *Department of the Navy Physical Security Instruction for Conventional Arms, Ammunition, and Explosives*
- **SCI:** DoDM 5105.21-Vol 1-3, *Sensitive Compartmented Information (SCI) Administrative Security Manual*
- **SAP:** DODM 5205.07 Volume 1-3, *DoD Special Access Program (SAP) Security Manual: Physical Security*
  - **IC Tech Spec-for ICD/ICS 705, *Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities***
- **Classified Materials (Secret and above)/Classified Communication Systems:** SECNAVINST 5510.36B DON Information Security Program – Points to DOD Manual 5200.01 DOD Information Security Program

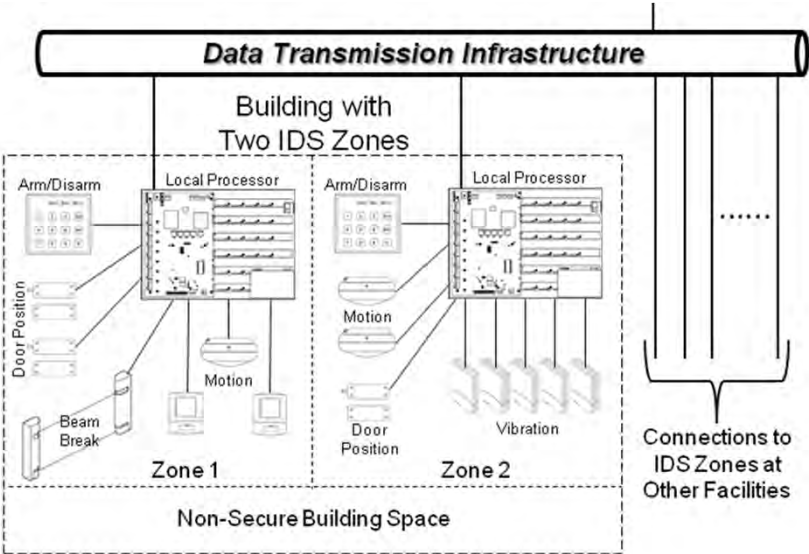
## Establishing the Requirement for ESS

- **The requirements for ESS must be established during the project planning stage.**
- **Establish an interdisciplinary planning team with local considerations to include the following:**
  - Planning
  - Supported Command
  - Site Security Manager (SSM) (when require for SCIF/SAPF)
  - Communications
  - Security: Installation/Region N3
  - Engineering

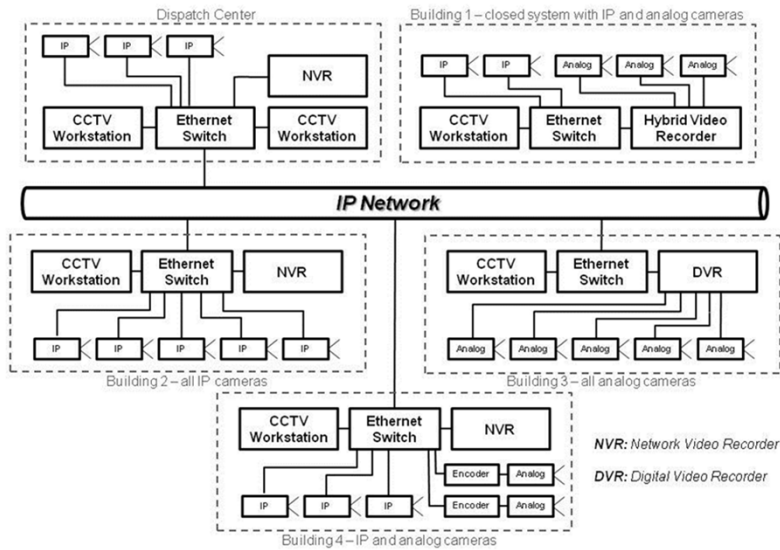
# Project Development

- The planning team must:
  - Determine what assets require protection
  - Understand related DoD/Service policy/regulations
  - Understand the objectives of the system
  - Understand the facility and user’s operational requirements and limitations.
  - Understand the security force’s capabilities
  - Incorporate ESS and related costs in project scope and budget.

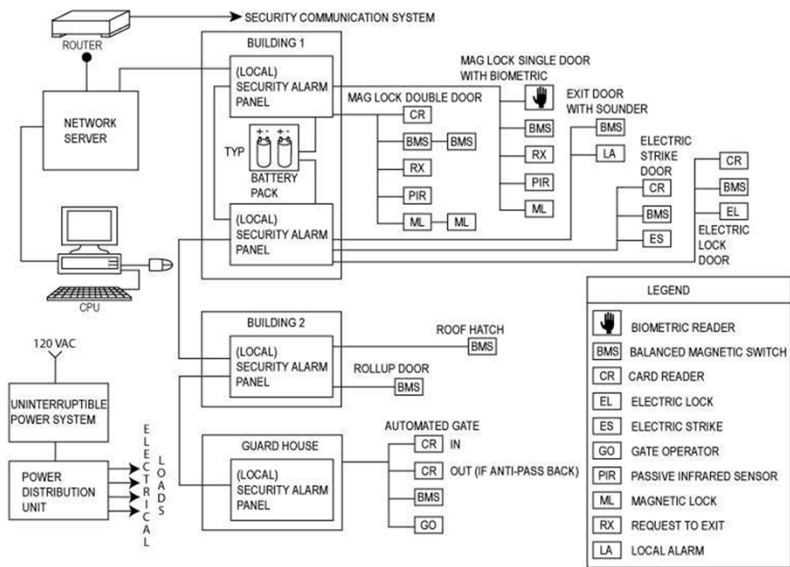
## Intrusion Detection System (IDS)



# Closed Circuit Television (CCTV) (Video Surveillance)



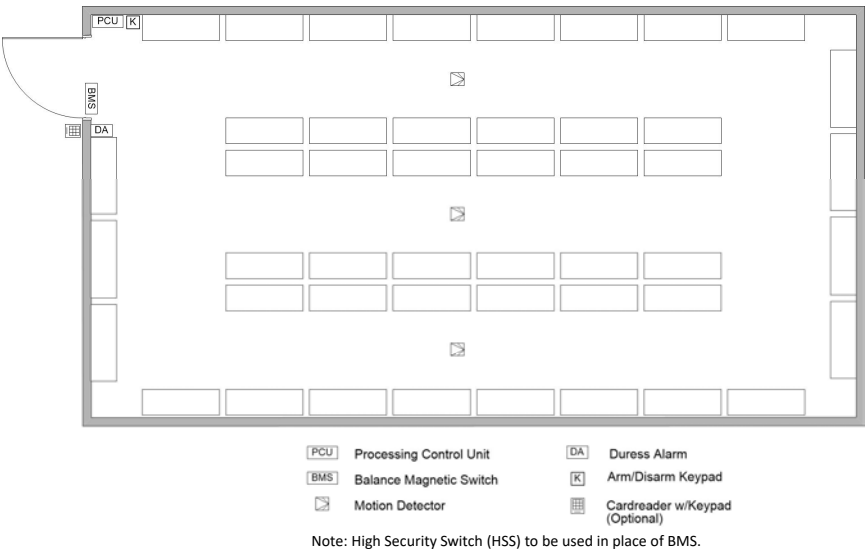
# Access Control System (ACS)



## AA&E Policy Base Requirements

- All perimeter doors and man-passable openings into the storage area shall be protected by High Security Switch (HSS) and a motion detection sensor.
- Duress alarm at all issue ports.
- Keypad at entrance and for all separated (unit-based) interior storage areas that require an independent IDS capability.
- Perimeter emergency exit doors shall be secured, alarmed, and monitored 24 hours per day.
- IDS shall be installed in accordance with UL 681 and consist of:
  - Level 2 high security switches (HSS) that meet UL 634, and/or other government approved sensors.
  - Motion detection sensors UL 639 listed.
- Premise Control Units (PCUs) shall be located within the protected area.

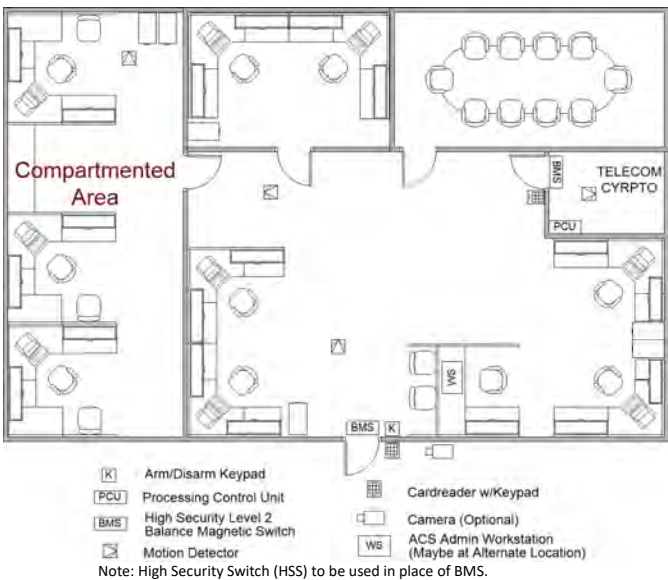
## Notional Layout: Arms Storage



## SCIF/SAPF Policy Base Requirements

- Perimeter doors shall be protected by High Security Switch (HSS) and a motion detecting sensor.
- Emergency exit doors shall be secured, alarmed, and monitored 24 hours per day.
- Interior areas through which reasonable access could be gained such as walls, doors, or windows shall be protected by an IDS.
- IDS shall be installed in accordance with UL 681 and consist of:
  - Level 2 high security switches (HSS) that meet UL 634, and/or other government approved sensors
  - Motion detection sensors that meet UL 639 listed, or approved by the CSA. Dual-Technology Sensors are authorized when each technology transmits alarm conditions independent of the other technology.
- Locate Premise Control Unit (PCU) within the space

## Notional Layout: SCIF or SAPF

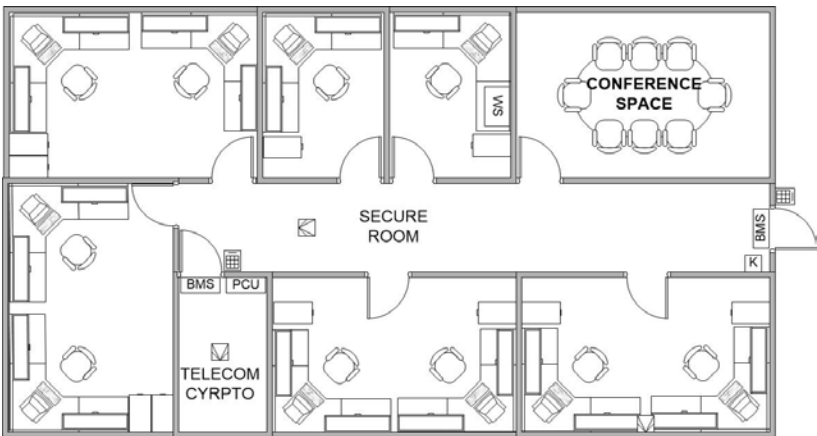




## Top Secret (TS) Policy Base Requirements

- All perimeter doors and man-passable openings into the secure area shall be protected by High Security Switch (HSS) and a motion detection sensor.
- Keypad at Primary Entrance.
- Perimeter emergency exit doors shall be secured, alarmed, and monitored 24 hours per day.
- IDS shall be installed in accordance with UL 681 and consist of:
  - Level 2 high security switches (HSS) that meet UL 634, and/or other government approved sensors.
  - Motion detection sensors UL 639 listed. Dual-Technology Sensors are authorized when each technology transmits alarm conditions independent of the other technology.
- Premise Control Units (PCUs) shall be located within the protected area.

## Notional Layout: Top Secret/Secret Open Storage



PCU	Processing Control Unit		Cardreader w/Keypad
BMS	High Security Level 2 Balance Magnetic Switch		Arm/Disarm Keypad
	Motion Detector		ACS Admin Workstation (Maybe at Alternate Location)

Note: High Security Switch (HSS) to be used in place of BMS.

## Word of Caution!

Don't go Crazy!



## Historical Timeline

- **FY04: NAVFAC assumed responsibility of the Navy's shore facilities Physical Security Equipment (PSE) Program (ATFP Ashore).**
  - Base Development will provide overall program management.
  - Naval Facilities Engineering Service Center (NFESC) was assigned as Deputy Program Manager (DPM) for the PSE Program. As the PSE DPM, NFESC has overall responsibility for the management, coordination, implementation and sustainment strategies for PSE.
- **FY06: Capital Improvements has accepted the responsibility for planning, design, installation, testing, and acceptance of Physical Security Equipment (PSE) associated with MCON projects.**
  - NFESC continued to maintain Program Execution oversight and was available for technical and acquisition support.
- **FY10: NAVFAC HQ CI assumed the program execution and oversight from NAVFAC EXWC. (Formally NFESC)**
- **FY21: NAVFAC ATFP Ashore Program transitioned and realigned from NAVFAC to CNIC and is now CNIC N6S Pubic Safety Systems (Formerly CNIC N3S).**
  - Work with CNIC N34 Force Protection/NEPPO Electronic Security Systems Branch



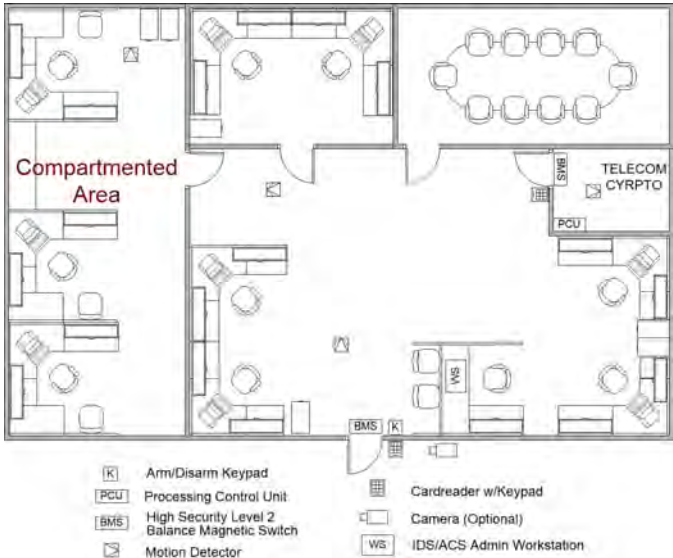
## ESS for Navy MCON

- **Military Construction for Navy (MCON):** For FY06 MCON projects and beyond, NAVFAC's goal, was to fully integrate the design, procurement, installation and testing of Electronic Security Systems (ESS) into MCON design and construction contracts.
  - **MCON/MCNR project funds procure the supporting infrastructure.**
  - **OPN or O&M funds procure, install and test the equipment.**
  - **ESS for MILCON does not include any exterior or perimeter ESS.**

## Electronic Security System (ESS) Equipment

- **CNIC N6S Public Safety Systems Program** addresses Physical Security Equipment requirements and funding for Electronic Security System (ESS) Equipment associated with Navy MCON.
  - **Per OPNAVINST 11010.20J:** CNIC N6S Program may provide funding for the ESS related to **Navy "Blue" MCON** when required for the protection of critical assets.
  - Justification is be based on DoD, SECNAV or OPNAV policy, not the supported command's operational preferences.
  - In the case of a SCIF, armory, top secret open storage or similar spaces, CNIC N6S may fund processing control unit, point sensors at the perimeter access points, volumetric sensors within the space, card readers and video assessment (CCTV) at the perimeter access points.
  - **In general, CNIC N6S will not fund card readers for compartmented areas within the space or exterior surveillance or fence line (perimeter) electronic security systems.**

## ESS Funding



## ESS Funding

- **Refer to PDC-04-02.09 (formerly BPMS B-1.3) Operational Outfitting Considerations**
- Types of projects typically funded under the CNIC N6S Program include assets such as:
  - Arms, Ammunitions, and Explosives (AA&E)
  - Sensitive Compartmented Information (SCI)
  - Special Access Program Information(SAPI)
  - Classified Materials (Secret and above)
  - Classified Communication Systems
    - Secret Internet Protocol Router Network (SIPRNet)
    - Joint Worldwide Intelligence Communications System (JWICS)

## ESS Funding

- Types of facility projects or programs that may require ESS, but are not funded by the CNIC N6S program include:
  - Marine Corps and Marine Corps Reserve Facilities
  - SOCOM
  - Missile Defense Agency
  - Strategic Systems Program (SSP)
  - Strategic Weapons Facilities (SWF)
  - Base Realignment and Closure (BRAC) Projects
  - Bachelor Quarters
  - Medical Facilities
  - Housing
  - MWR and Retail Facilities
  - ECF/ACP

## ESS Funding

- For Marine Corps, Army, Air Force and other Defense Agency projects:
  - Coordinate the PSE, ESS and IDS requirements and funding with the resource sponsor and/or supported command's representative
  - **Provide empty conduit systems for PSE with MILCON Design and Construction.**
  - Agency's PSE Program provides the design, installation and testing of the Physical Security Equipment.

## ESS Funding

- **OPNAVINST 11010.20J: ESS infrastructure efforts are considered “Real Property” and can be funded with project funds regardless of funding source.**
  - Interior infrastructure includes conduit, junction boxes, electronic door strikes, door hardware, mounting hardware, and power connections.
  - Exterior infrastructure includes items such as exterior duct banks, manholes, utility poles, exterior communication cabling, and power connections.

## ESS Funding for MILCON

- **OPNAVINST 11010.20J: ESS is classified as “Personal Property” and cannot be funded with Military Construction (MILCON) dollars.**
  - Equipment (Active Devices) includes items such as central processing units, control panels, interior sensors, exterior sensors, cameras, monitors, and the interior communications cabling connecting these devices together.
- **Resource sponsor for equipment varies based on service and program management.**

## OPNAVINST 11010.20J Property Classification

- **Real Property/Installed Equipment/Built-In Equipment:** Real Property Installed Equipment (also known as installed equipment or built-in equipment).
  - Equipment or fixtures **permanently attached** to or built into a real property facility, which are essential to or an integral part of the facility and therefore typically engineered into the final design and construction of the facility.
  - Real property equipment is considered part of the facility and **not intended to be moved outside the facility envelope**. The removal of this equipment might substantially damage the facility or render the facility unusable.
  - Real property equipment work must adhere to all legislation, regulations and policy applicable to real property facilities (unless otherwise stated).
- **Personal Property. Accessory equipment and furnishings that are movable in nature and not affixed as an integral part of a real property facility.**
  - **Personal property includes operational equipment that is detachable without damage to the real property facility or real property equipment.**
  - **Personal property is not required for the operation of the real property facility but is required for the functional operation and activities utilizing the real property facility.**
- **FUNDING OF: Personal property procurement and installation must be financed from applicable O&M appropriations, RDT&E appropriations, family housing appropriation, procurement appropriations, and OPN or DWCF resources, as appropriate.**

**NOTES**  
1. See COMNAVFACENGSSYSCOM portal under "Asset Management" for latest additions and updates to this property classification table. See Chapter 1, subparagraph 2b(7).

## OPNAVINST 11010.20J Appendix A Property Classification Table

Item (Note 1)	Real Property, Installed and Built In Equipment	Personal Property or Collateral Equipment
Security and Antiterrorism Related		
Waterfront boat barriers (including anchors)		X
Electronic Harbor Security System		X
Access control islands for gate entry	X	
Gates and turnstiles (built in)	X	
Active vehicle barriers (built-in)	X	
Passive vehicle barriers (built-in)	X	
Traffic control drop arms (built-in)	X	
Guard booths, overwatch and firing positions (built in)	X	
Under-vehicle (in-ground) integrated inspection equipment		X
Fencing	X	
Outdoor camera poles and towers	X	
Explosive and contraband detection systems		X
ESS infrastructure to include conduit, junction boxes and power connections	X	
ESS equipment for the following: intrusion detection system, access control systems and video assessment and surveillance systems sometimes referred to as closed-circuit television		X
Closed-circuit television system for child development center, SAC or youth center child abuse prevention		X
Door locks (cipher or combination locks, including magnetic and electronic strike)	X	
Sound masking equipment for sensitive compartmented information facilities		X
Protected distribution system	X	
Warning globes for sensitive compartmented information facilities		X
Interior mass notification system	X	

**NOTE FROM TABLE**  
1. See COMNAVFACENGSSYSCOM portal under "Asset Management" for latest additions and updates to this property classification table. See Chapter 1, subparagraph 2b(7).



## Project Development

- **The requirements for a secure facility or space must be established during project planning.**
- **Establish an interdisciplinary planning team with local considerations to include the following:**
  - Planning
  - Supported Command
  - Supported Command's Security Manager
  - Communications
  - Security: Installation/Region N3
  - Engineering
- **PM/DMs need to proactively engage the Supported Command and their Security Manager to coordinate project security requirements.**



## Project Development

- **The planning team must:**
  - **Determine if there is the regulatory requirement for ESS.**
    - Determine what assets require protection.
    - Understand related DoD/Service policy/regulations.
  - **Determine if the supported command will want more than the regulatory requirement.**
  - **Determine funding source(s) for electronic security systems.**
    - CNIC N6S?
    - Supported Command?

### Project Development

- **Document the ESS requirements**
  - Block 10 (scope) of DD 1391 and backup documentation should be utilized to describe ESS requirements/Assets.
    - Does this facility contain critical assets?
      - AA&E?
      - SCI?
      - SAP?
      - Classified Information/Equipment?
      - COMSEC material?
  - Utilize 1391 Team Checklist to help document requirements

### 1391 Team Checklist – Physical Security

ID#	Keyword	Item
4.03	Security system	Coordinate Electronic Security Systems (ESS) / Physical Security Equipment (PSE) including Intrusion Detection Systems (IDS) with NAVFACHQ CI ATRP, User/Operator, and Installation's BCO.
7.12	SCIF	Determine whether this project will need to include a Sensitive Compartmented Information Facility (SCIF) or a Special Access Program Facility (SAPF). SCIFs and SAPFs have special security requirements such as opening restrictions, special walls, and sound attenuation. For each SCIF or SAPF the following information should be provided: <ul style="list-style-type: none"><li>- SCIF ID# assigned by Accrediting Official (AO) or SAPF ID#</li><li>- Space requirement (square feet)</li><li>- Site Security Manager (SSM) contact information (name, phone#, email)</li><li>- SCIF/SAPF Preliminary Construction Security Plan (CSP)</li></ul>
7.13	Control access	Determine if this project requires a Controlled Access Area (CAA) other than a SCIF or SAPF within the facility. If so, indicate the number and square footage of each CAA.

## Project Development

### Document the Cost Associated with Physical Security Requirements

- **Block 9 (Project Cost) of DD 1391 and backup documentation should be utilized to document costs of the PSE requirements.**
  - Cost for PSE infrastructure must be included in Block 9 of the DD 1391 under primary facilities (Built-in Equipment).
  - Cost for PSE (Actual Equipment) must be included in block 9 of the DD 1391 under “Equipment Under Other Appropriations.”
  - **Remember: Equipment cannot be paid for with Military Construction funds.**

## Project Development

### Tools for Establishing Budgets for ESS

- **ESS Budget Estimator:**
  - Excel Spreadsheet intended to provide DoD facility planners, cost estimators and designers a unified method of budgeting for Electronic Security Systems for facilities. **This tool is intended to be used for budget estimating only and work within OSD and DD 1391 guidelines.** Tool will output budget cost for ESS equipment and the associated infrastructure.
- **Gate Automation Equipment Estimator:**
  - Excel Spreadsheet intended to provide DoD facility planners, cost estimators and designers a unified method of budgeting for Gate Automation equipment only. This tool does not provide infrastructure costs.



## ESS Budget Estimator

1.Component		Military Construction Program		2. Date	
Navy		Electronic Security Systems (ESS) Budget Estimator Ver 1.0		2/6/2008	
3. Installation and Location/UIC			4. Project Title		
ANYWHERE USA			ESS Project EXAMPLE		
5. Category Code		6. Project Number	7. User Defined	8.User Defined	
9. User Input					
Facility					
A. Enter the size of the facility in square feet.				10,000	
B. Enter the number of floors.				3	
C. Does this project include exterior (building façade) access control (i.e. card readers at exterior doors into the facility)? Enter Yes or No.				Yes	
D. Does this project include interior volumetric sensors (i.e. interior mounted motion detectors) in areas other than the interior CAA's or SCIF's? Enter Yes or No.				No	
E. Does this project include interior closed circuit TV in areas other than the interior CAA's or SCIF's? Enter Yes or No.				No	
Building Perimeter					
F. Does this project include exterior (building façade) volumetric sensors (i.e. exterior mounted motion detectors protecting critical exterior assets)? Enter Yes or No.				No	
G. Does this project include exterior (building façade) closed circuit TV (i.e. building mounted cameras viewing exterior doors and around the building)? Enter Yes or No.				Yes	



## ESS Budget Estimator

Site Perimeter	
H. Does this project include exterior (site perimeter) access control (i.e. card readers at perimeter vehicle or pedestrian gates)? Enter Yes or No.	No
I. Does this project include exterior (site perimeter) intrusion detection (i.e. buried or fence mounted intrusion sensors)? Enter Yes or No.	No
J. Does this project include exterior (site perimeter) closed circuit TV (i.e. cameras viewing perimeter boundary of site)? Enter Yes or No.	No
K. Enter length of perimeter fence to be protected in linear feet.	0
Interior Enclaves	
L. Does this project include interior Sensitive Compartmented Information Facility's (SCIF's)? How many?	2
M. Enter the average size of the interior SCIF's in square feet.	400
N. Does this project include interior Controlled Access Areas (CAA's) in addition to SCIF's? How many?	1
O. Enter the average size of the interior CAA's in square feet.	450
Site Specifics	
P. Does this project include local monitoring (at the facility) or remote monitoring (at a central monitoring station) of the electronic security system? Enter Locally, Remotely, or Both.	Both
Q. Does this project warrant biometric devices for access control? Enter Yes or No.	No
R. Does this project warrant thermal imaging for the closed circuit television cameras? Enter Yes or No.	No
S. Does this project warrant video analytics/video content analysis for perimeter intrusion detection? Enter Yes or No*	No
T. What is the overall Level of Protection requirement of the facility? Enter Low, Medium, or High.	Low



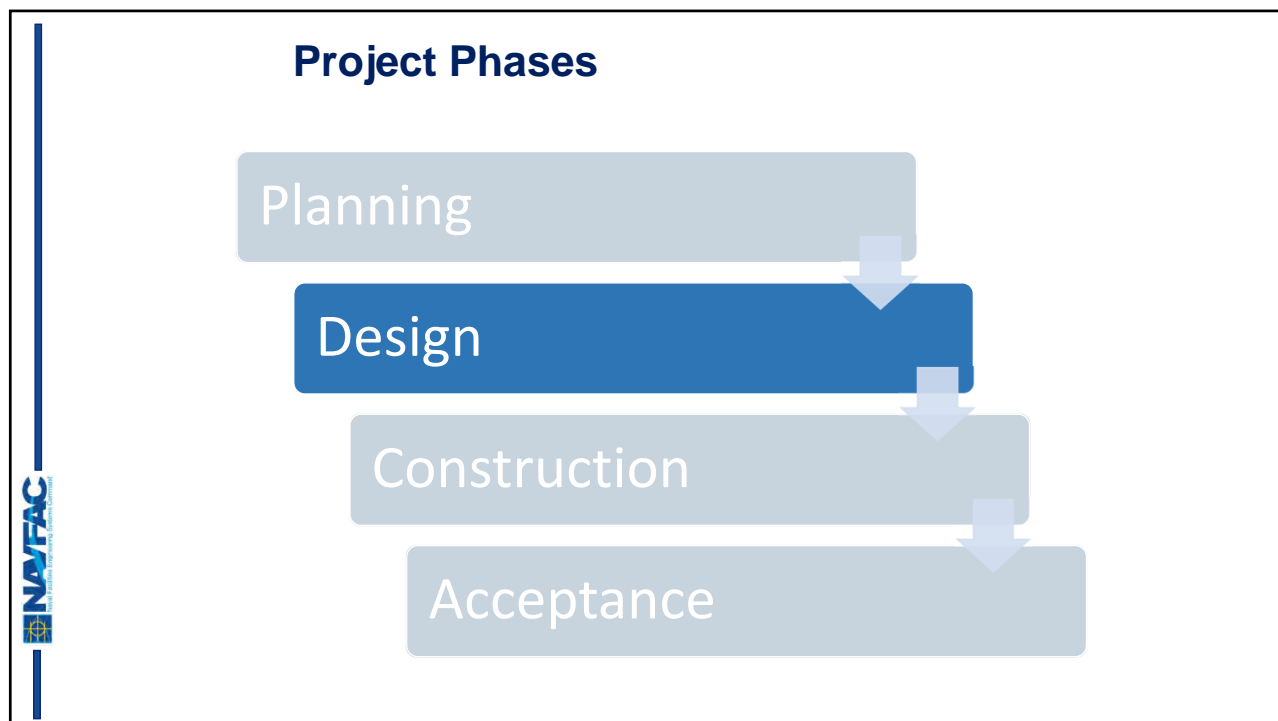
## ESS Budget Estimator (Output)

COST ESTIMATE			
System	Supporting Infrastructure	PSE Equipment	Total
Controlled Access Areas	4,345	14,842	19,187
Sensitive Compartmented Information Facilities	50,281	80,001	130,282
Interior Intrusion Detection Zones	0	0	0
Interior Closed Circuit Television Zones	0	0	0
Exterior (Bldg Façade) Access Control Zones	4,212	9,627	13,840
Exterior (Bldg Façade) Intrusion Detection Zones	0	0	0
Exterior (Bldg Façade) CCTV Zones	2,852	3,842	6,694
Perimeter Access Control Zones	0	0	0
Perimeter Intrusion Detection Zones	0	0	0
Perimeter Closed Circuit Television Zones	0	0	0
Biometric Access Control Zones	0	0	0
Thermal Imaging Zones	0	0	0
Video Analytic Zones	0	0	0
Exterior (Bldg Façade) Monitored Door Zones	0	0	0
ACS Local Monitoring Zones	1,492	7,964	9,456
CCTV Local Monitoring Zones	2,985	19,617	22,602
ACS Remote Monitoring Zones	2,985	14,843	17,828
CCTV Remote Monitoring Zones	5,970	48,124	54,093
<b>SUBTOTAL</b>	<b>75,122</b>	<b>198,660</b>	<b>273,982</b>
<b>User input (only applied to PSE Equipment)</b>			
1. ACF	0.94	-11,002	
2. Contingency	10.0%	18,693	
3. SIOH	8.0%	16,450	
4. Escalation	1.15	33,311	
<b>User input (for OCONUS Mobilization/Per Diem)</b>			
5. OCONUS	\$	0	
<b>TOTAL</b>	<b>75,122</b>	<b>255,382</b>	<b>330,504</b>
Total OP Request	\$	255,381.90	
Total MILCON Request	\$	75,121.75	



## Gate Automation Equipment Estimator

Gate Automation Budget Estimator (Ver 12.07)		
Estimated by:	Your Name	
Project Title:	Main Gate	
Project Location:	NAVSTA Anywhere	
Project Number:	P-XXX	
Fiscal Year:	FY10	
Date:	12/14/2007	
ACF:	0.94	
Escalation:	1.15	
Number of Gates	1	
Number in Ingress Lanes	4	
Number of Egress Lanes	2	
Number of Pedestrian Gates	1	
Number of Security Dispatch Stations	1	
Number of Badging Stations	2	
Number of Badges/Assets	1000	
Equipment Cost		\$251,607
System Design Cost		\$25,161
System Install/Programming Cost		\$75,482
Integration, Testing, & Training		\$35,225
Subtotal:		\$387,474
ACF Adjustment:		\$364,226
Escalation:		\$418,860
Contingency (5.0%):		\$20,943
Total Contract Cost:		\$439,803
SIOH (8.0%):		\$35,184
Subtotal:		\$474,987
<b>Total OPN Funding Request :</b>		<b>\$480,000</b>



### General Design Strategy

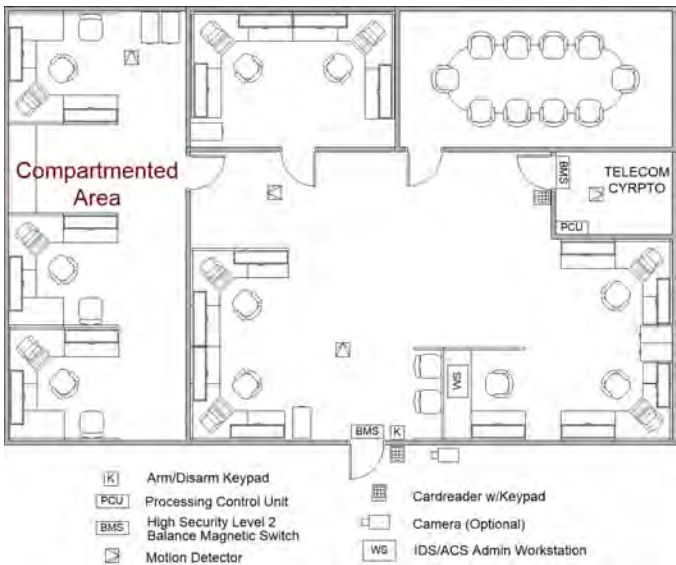
- **Intrusion Detection System**
  - All Interior areas of a protected area through which reasonable access could be gained shall be protected by IDS, unless continuously occupied.
    - If the occupants of a continuously occupied space cannot observe all potential entrances, the space shall be equipped with a system to alert occupants of intrusions into the protected area.
  - Emergency exit doors shall be monitored 24 hours a day to provide quick identification and response to the appropriate door when there is an alarm indication.

On the left side of the slide, there is a vertical blue line with the 'NAFAC' logo and a small yellow square icon at the bottom.


## General Design Strategy

- **CNIC N6S is not resourced or authorized to fund 100% coverage of volumetric sensors when there is security in-depth and reasonable access is low.**
  - Volumetric sensors should be placed to protect doors and then strategically placed in the hallways leading up to or in the rooms where the secure assets are being stored, and where the crypto gear is located in the Secure Area.
- **CNIC N6S will not fund card readers for compartmented areas within the space, exterior surveillance, or fence line (perimeter) electronic security systems.**

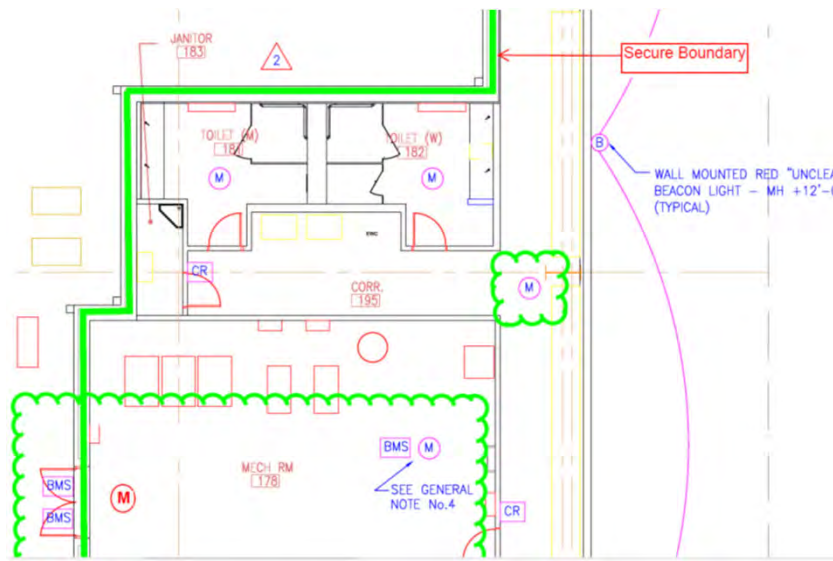
## Notional Layout







# Remember: Don't go Crazy!



The diagram is a floor plan of a facility. It includes several rooms: JANITOR (183), TOILET (RM) (182), TOILET (W) (182), CORR. (195), and MECH. RM (178). There are also several rooms marked with 'M' (Mechanical) and 'BMS' (Building Management System). A green dashed line outlines a perimeter, and a red dashed line outlines a 'Secure Boundary'. A blue line indicates a 'WALL MOUNTED RED "UNCLE" BEACON LIGHT - MH +12'-6" (TYPICAL)'. A note points to a room: 'SEE GENERAL NOTE No.4'. A red triangle with the number '2' is located near the JANITOR room. A red circle with the letter 'M' is located near the MECH. RM. A red circle with the letter 'B' is located near the 'Secure Boundary'.



# Roles and Responsibilities



The illustration shows a group of blue 3D human figures standing around a large puzzle. The puzzle is composed of several pieces, with one piece being red, one being green, and one being yellow. The figures are holding the puzzle pieces, symbolizing teamwork and shared responsibility.

## **Program Roles and Responsibilities**

### **▪ Project Team:**

#### **▪ Planning/DD1391 Development**

- Coordinate with supported command to establish requirement for ESS (Program Manager to validate requirement and funding)
- Program for ESS infrastructure
- Include the appropriate OP or O&M cost
- Determine appropriate fund source and procurement strategy for ESS
  - CNIC N6S or Supported Command
  - Option(s) to contract

## **Program Roles and Responsibilities**

### **▪ Project Team (cont.)**

#### **▪ Project design**

- Validate planning criteria
- Coordinate with supported command, security POC to refine ESS requirements.
- Include ESS infrastructure to support equipment

## PDC-04-02.09 formerly (BPMS B-1.3) Operational Outfitting Considerations

- **Project Manager responsibilities:**

- Coordinate/submit the scope, funding and schedule requirements for the ESS to the CNIC N6S Program Manager for programming.
- For ESS that is not a policy based requirement or not supported by the CNIC N6S Program, coordinate funding with supported command.
- Include ESS infrastructure in MCON/MCNR.
- ~~Include the procurement, installation, and testing of ESS equipment as an option to the MCON project.~~
- Coordinate and request the OPN ESS funds from CNIC N6S or supported command, when required.
- Coordinate the design schedule with the supported command's site security manager to ensure timely reviews.
- Ensure the supported command Coordinates ESS with NIWC LANT to justify the requirement.
- Coordinate the inclusion of infrastructure (empty conduit system with pull wire and power connections) to support the required ESS equipment.
- Coordinate the design schedule with NIWC LANT and the supported command's site security manager to ensure timely reviews.
- Contact CNIC POC if there are schedule impacts due to coordination issues with NIWC LANT.

## PDC-04-02.09 formerly (BPMS B-1.3) Operational Outfitting Considerations

- **Design Manger:**

- Coordinate design of ESS infrastructure with NIWC LANT
- Do not include infrastructure for ESS that has not been validated by NIWC LANT.
- Coordinate any scope and cost issues with the Project Manager.

- **Construction Manager:**

- Coordinate the construction schedule with NIWC LANT and site security manager to ensure timely installation of ESS.

- **NIWC LANT Project Manager:**

- Coordinate ESS requirements and budget with supported command and CNIC.
- Provide Designer of Record preliminary ESS layouts and one-line diagrams to include in the construction project solicitation documents.
- Review design submittals to insure coordination with equipment installation.

## CNIC N6S Funding

- **When requesting funds from CNIC N6S, provide:**
  - **Justification that project falls under CNIC N6S.**
  - **Drawings with ESS equipment layout**
  - **Cost Estimate**
  - **Funding Request**



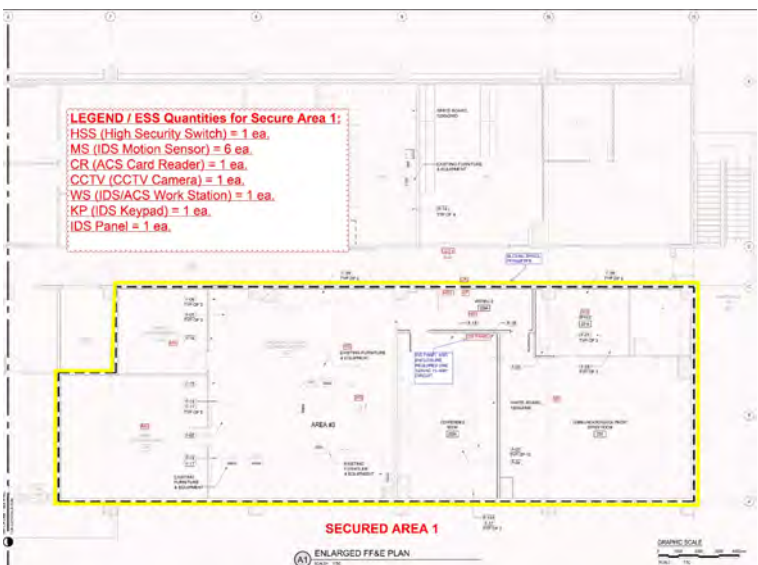
## CNIC N6S MCON ESS Guidance to the Field Activities

- **Justification:**
  - **Verify the project is a Navy “Blue” MCON.**
  - **Verify the asset being protected and the associated regulatory guidance or policy generates the requirement.**
  - **Arms, Ammunitions, and Explosives (AA&E)**
  - **Classified Materials (Secret and above)**
  - **Classified Communications System**
    - SIPRNet
    - JWICS
  - **Sensitive Compartmented Information (SCI)**
  - **Special Access Program Information (SAPI)**

## CNIC N6S MCON ESS Guidance to the Field Activities

- Drawings with ESS equipment layout:
  - Floor plan clearly delineating the protected area(s) and equipment CNIC N6S is expected to fund to include:
    - The perimeter of the space(s) highlighted
    - Location of processing control unit (PCU) within the space.
    - Location of perimeter point sensors and volumetric sensors within the space.
    - Location of card reader with key pad and camera (optional) at the primary entrance
    - Location of Arm/Disarm keypad within the space
    - Location of Access Control Workstation
    - Table summarizing the types and quantities of ESS equipment proposed to be funded by CNIC N6S

## CNIC N6S MCON ESS Guidance to the Field Activities





## **CNIC N6S MCON ESS Submission, Review, Approval & Fund**

- CNIC N6S uses the drawing submission to perform a preliminary review of the ESS.
  - Ensures the drawings are consistent with the guidance provided in NAVFAC BMS B-1.3 Section 1.3.2 Perform Coordination for Electronic Security System (ESS) Equipment Procurement and Installation, and the notional layouts in UFC 4-021-02 Appendix C.
  - CNIC N6S provides initial recommendations to facilitate drawing package approval and focuses on the layout of the secure perimeter and the baseline ESS.
    - ONLY One (1) PCU, Card Reader and Key Pad, and Camera per secure area, and BMSs and volumetric sensors covering each door and man passible opening along the secure perimeter.
    - Volumetric sensors strategically placed within the Protected Area (not 100% Coverage)
  - Submitting drawings that are not consistent with the baseline requirements will add significant time to the review process.



## **CNIC N6S MCON ESS Submission, Review, Approval & Fund**

- After the Preliminary Review and submission of updated drawing package, CNIC N6S performs a formal detailed review and validation.
  - PM to provide drawings with CNIC N6S recommendations incorporated.
    - Each drawing page is to include a table indicating quantities of ESS equipment.
  - CNIC N6S performs a detailed review of the drawings based on the Policy Baseline for the type of secure area.
    - CNIC N6S Reviewer will provide comments to PM for resolution.
  - The PM updates the drawings and provides responses to the comments that will form part of the project submission.
  - CNIC N6S and PM resolve the comments and reach concurrence on the types/quantities of the ESS to be funded by CNIC N6S.

## **CNIC N6S MCON ESS Guidance to the Field Activities**

- **Cost Estimate:**
  - Budget Estimate for DB Projects
  - Cost Estimate for DBB Projects
    - Cost estimate does not need to be completed until CNIC N6S validates the funding requirement.
- **What CNIC N6S does not fund and is the responsibility of the Base/Supported Command/End User.**
  - Anything above the policy based requirement
  - Equipment exterior to the facility to connect to the base system to include in the central monitoring station
  - Any certifications to include accreditation and cybersecurity certifications
  - Follow-on sustainment/maintenance of the ESS

## **CNIC N6S MCON ESS Submission, Review, Approval & Fund**

- After resolution of Cost Estimate, FEC PM sends the Final Project Submission to CNIC N6S which includes the Final Drawings, Cost Estimate and E-mail with resolution of comments.
- Final project package submission will be forwarded to the CNIC N6S PS/AC APM for final review/approval. Includes the following documentation:
  - Final project submission documents from the FEC PM.
  - Recommendation for approval with detailed summary from CNIC N6S reviewer.
- CNIC N6S PS/AC APM reviews Final Project Submission and Summary from the CNIC N6S review and provides notification of approval.





## **CNIC N6S MCON ESS Submission, Review, Approval & Fund**

- Proceed to funding of the project after CNIC N6S PS/AC APM approval.
  - CNIC N6S provides guidance to the FEC PM for completion and submission of a formal funding request through the NAVFAC e-Tracker System and for back-up documentation, e.g., contractor's proposal, to be provided separately to justify that the funds being requested are for the approved quantities of ESS.
  - Upon request, CNIC N6S will provide Promise-to-Pay to the FEC PM to facilitate issuance of an RFP and award of the Option.
  - FEC PM completes and submits the formal funding request in the NAVFAC e-Tracker System based on the amount for the Option and submits back-up documentation in e-mail to the CNIC N6S PS/AC APM and BFM. Total funding request includes amount for award of Option plus 8% for FEC supervision & administration (for OPN funded projects per NAVFAC HQ).
  - Upon approval of the funding request, CNIC N6S coordinates issuance of project funds to the FEC for award/execution of the Option for the MCON ESS Project.



## **General Construction Coordination**

- **Construction Manager:**
  - **Coordinating required ESS infrastructure prior to equipment installation**
  - **Coordinate site surveys for ESS contractor when separate from prime contract**
  - **Coordinate the construction schedule with the supported command's site security manager:**
    - Coordinate site surveys by Site Security Manager when required for SCIF, SAPF, and Secure spaces
    - Recommend site security manager be invited to attend Design-Build (DB) Post Award Kickoff (PAK) or Design-Bid-Build (DBB) Pre-Construction Conference (PreCon).
  - **Ensure timely on-site inspection, testing, training, and acceptance of ESS, as required.**

## **CNIC N6S MCON ESS Common Concerns and Questions**

- **What will CNIC N6S Fund ?**
  - ESS for Navy MCON based on DoD, SECNAV or OPNAV Policy/Regulatory requirements.
- **Who does the Design ?**
  - Designer of Record provides system layout and major elements with location in sufficient detail to design the infrastructure required (power, conduits, etc).
  - Designer of Record provides specification UFGS 28 10 05 Electronic Security System (ESS) and UFGS 28 08 10 Electronic Security System Acceptance Testing.
    - UFC 4-021-02 provides sufficient detail to design the system.
    - DoD, DNI, SECNAV and OPNAV manuals and instructions provide baseline requirements.
- **Who funds Design ?**
  - Infrastructure, equipment layout and equipment specifications are funded as part of the MCON project. (Designer of Record)

## **CNIC N6S MCON ESS Common Concerns and Questions – cont'd**

- **How to determine the budget cost?**
  - ESS Budget Estimator for DD1391 or DB RFP
  - ESS Cost Estimator for DBB.
- **Is building complete and useable without the ESS installed?**
  - Yes, building just needs to be occupied/guarded.

## **CNIC N6S MCON ESS Common Concerns and Questions – cont'd**

- **Are there special requirements associated with the installation of the infrastructure associated with ESS equipment for MCON Projects?**
  - Only for SCI & SAP: Must be U.S. Company using U.S. Citizen
- **Are there special requirements associated with the installation and testing of ESS equipment for MCON Projects?**
  - **Depends on the location and asset:**
    - AA&E has no special requirement
    - Classified Information within the U.S.: U.S. Citizen with a trustworthiness determination (DBIDS or NCACS credential)
    - SCIF & SAPF within the U.S.: U.S. Company using U.S. Citizen
    - SCI & SAP outside U.S.: Top Secret-cleared, Secret-cleared.
- **Contained in UFGS 01 14 00 Work Restrictions**

## **NAVFAC Take Away**

- **As a construction agent for the Department of Defense, we must understand the requirements for ESS and ensure that the projects we plan, design, and construct meet the policy based accreditation requirements.**
- **Be Proactive: Find out who is the designated Site Security Manager for SCIF and SAPF.**
  - **Get them involved early in the project planning.**
  - **Keep them involved throughout the project.**

## Supported Command's Take Away

- **NAVAFAC needs your input during the entire process (planning, design and construction).**
- **Be Proactive: For SCIF and SAPF assign a Site Security Manager during the planning phase and ensure their involvement throughout the project – planning through construction/accreditation.**
  - Provide the project requirements to NAVAFAC as early in the process as possible.
  - Make sure the designer of record understands the project security requirements.
  - Review submittals.
  - Attend planning, design and construction meetings.
  - Get involved and keep involved throughout the project.



## Thanks!

### NAVFAC PDCC:

**John Lynch, PE**  
[john.j.lynch8.civ@us.navy.mil](mailto:john.j.lynch8.civ@us.navy.mil)  
**(757) 322-4207**

**Julie Heup, PE**  
[julie.m.heup.civ@us.navy.mil](mailto:julie.m.heup.civ@us.navy.mil)  
**(757) 322-4447**

