Expanding Role of IT in Enterprise Electronic Security Systems

White Paper | June 2021

M.C. DEAN AUTHORS

Eric Dean
Chief Technology Officer
Security & Electronic Systems

David Sealock
Vice President of Operations
Security & Electronic Systems

Expanding Role of IT in Enterprise Electronic Security Systems

Physical security employs physical protection methods such as fences, gates, barriers, and doors combined with electronic security methods including intrusion detection, video surveillance, and access control. Over the past decade, electronic security systems have evolved from standalone systems managing only physical assets into distributed, networked information technology (IT) systems integrated into security operations. Today's electronic security systems (ESS) employ a wide range of advanced enterprise information technology dedicated to protecting sensitive physical and IT assets. This cyber-physical evolution is shifting the paradigm of ESS technology and operating models due to the following:

- **Enterprise-wide threats**: Electronic security systems are an integral part of a defense in depth security architecture, including protecting and controlling access to computers, information systems, and other networked assets. Controlling physical access must be viewed within the context of the overall enterprise as opposed to a single location, consequently, a breach at a single location may impact the entire enterprise. This approach requires a shift in operations, enhancing reliance on Government-wide high assurance credentials and employment of advanced analytics, among other capabilities.

- **Advanced threat mitigation capabilities**: As the security threat environment continues to evolve, organizations responsible for electronic security will increasingly rely on the application of advanced technologies such as data analytics and artificial intelligence-enabled event correlation and analysis to identify and mitigate real time threats. The resources and expertise required to deploy and operate them are not always available at a local level, and the enterprise electronic security systems must network and integrate with cloud-based capabilities to leverage the most powerful analytics capabilities.

- **Continuously evolving cybersecurity requirements**: While electronic security systems often protect IT assets, ESS themselves are networked systems employing a broad range of IT components and technologies. They also must remain protected from cybersecurity threats and comply with FISMA requirements for federal systems. The National Institute of Standards and Technology (NIST) SP 800-37 Risk Management Framework provides guidelines and processes for organizations to manage risk by implementing administrative, operational, and technical information assurance controls with continuous monitoring. The physical and environment control family defined by the NIST SP 800-53 rev 5 and the Physical Access Control Systems (PACS) overlay provide for specific IT controls that apply to the PACS integrated with its network environment. Inadequate implementation of cybersecurity controls jeopardizes the authorization to operate (ATOs) of all Intelligence Community Directive (ICD) 705 spaces and IT assets within Department of Defense (DOD) facilities protected by noncompliant ESS.

Some of the current operational and technological challenges facing the ESS leadership include:

- Enterprise-wide implementation of high assurance credentials in accordance with maturing standards
- The need for federated local, regional, and enterprise operations capability
- Extensive integration requirements using secure communications
- Implementation of cybersecurity controls and Federal Information Security Management Act (FISMA) compliance

Implementation of High Assurance Credentials

In 2005, NIST created a credential standard called Federal Information Processing Standards (FIPS) 201 that mitigates the risks of a non-interoperable identity credential across the government. FIPS 201 relies upon Public Key Infrastructure (PKI) implementations within Federal Identity Credentialing and Access Management (FICAM)-certified PACS. FICAM certifies all integrated PACS components against FIPS 201

standards including electronic readers, electronic access control panels, certificate validation software, and access control software.

Earlier revisions of the FIPS 201 allowed authentication using the unsigned Card Holder Unique Identifier (CHUID). However, due to the methods' vulnerability to card cloning, the latest revision of the standard, FIPS 201-3, no longer allows for authentication using CHUID. NIST 800-53 also addresses concerns surrounding weak authentication in its Revision 5 Physical and Environmental Protection family of controls and supplemental Security Control Overlay, NIST 800-53 Rev 5 Security Controls for electronic Physical Access Control Systems (ePACS).

To meet the FIPS 201-3 high assurance requirements and to fully realize the benefits of the Government-wide credential standards, existing and new ESS systems will have to incorporate the following:

- **Reader and panel upgrades**: Many of the DOD's existing readers that support unsigned CHUID authentication will need to be replaced with high-assurance FIPS 201 readers capable of performing certificate-based authentication. Prior to 2021, DOD Common Access Cards (CACs) were not encoded with contactless card authentication key certificates. This change significantly impacts the DOD'S electronic access control infrastructure rendering much of it obsolete. In most cases, this process requires replacing the electronics panels with new panels that store FIPS 201 certificates that are interoperable FICAM certified readers.
- **Enterprise-wide enrollment and cardholder replication**: Without cardholder replication between PACS, personnel must stop at a visitor center and manually enroll their badge at every facility. This is a time-consuming process that undermines the benefits of using enterprise-wide high assurance credentials. Enterprise-wide or regionalized replication of cardholder databases and the associated certificate data is required to fully realize the benefit of federated credentials.
- **Support for certificate revocation validation**: To validate that a person's FIPS 201 CAC credential has not been digitally revoked, the FIPS 201 standard requires that each DOD PACS validate all credentials no less frequently than every 18 hours against the certificate revocation lists maintained by the DOD certificate authorities.
- **Internet-based connectivity to Federal Bridge to support credential interoperability**: To support full Government interoperability of credentials in accordance with the PIV standard, the participating PACS deployments must have access to the Internet-connected Federal Bridge, the participating PKI Certificate Authorities, and Certificate Revocation Lists.
- **Support for multiple assurance levels**: NIST 800-116 provides guidance on how to correctly design PIV and CAC security implementations within a facility. For example, perimeter or lobby entrances may support a contactless secure read using the contactless card authentication key certificate but access to a sensitive compartmented information facility (SCIF) may require CAC insertion with a pin or biometric authentication. The move towards multi-level authentication model within ESS will result in additional challenges during the design and implementation phases including but not limited to the following:
    - Requirements management to effectively map assurance level to each space/access portal;
    - Interface coordination to ensure sufficient networking and physical installation provisions to support the appropriate assurance level;
    - Maintaining installation effectiveness and efficiency in light of the growing number of configuration options

Federated Operating Model

The growing complexity and criticality of ESS necessitates a tiered operating model, which consists of a combination of an Enterprise Operations Center (EOC) capability and regional/local administration, as outlined below:

- **Centralized/regional operations function**: The centralized operations functions must focus on monitoring the electronic security *system as a whole*, and ensure its functionality, performance, availability, and reliability. These responsibilities include corrective and preventive maintenance on the entire security system, including but not limited to managing the Microsoft Windows domain infrastructure and services, (virtualized) enterprise network functions, management of public and enterprise digital certificates, enterprise integrations, and, crucially, cybersecurity controls and related functions.
- **Local administration**: The local administration capability is required to effectively administer access privileges at the facility and individual room/space level. While the local administrators will not have advanced systems management privileges or the ability to enroll credentials, they must have *exclusive* management access to their respective spaces based on the established requirements and validated operational needs / need to know.

Implementation of Cybersecurity Controls and FISMA Compliance

Deploying electronic security systems on standalone networks undermines the ability to implement strong authentication capabilities, robust logging and auditing functions, system integrity controls, such as malware protection, configuration management, patching, and other information assurance controls.

All ESS deployments must have a comprehensive approach to implementing or inheriting from the existing authorized government networks all required NIST SP 800-53 controls. Furthermore, the implementation of such cybersecurity controls must extend beyond the traditional IT infrastructure level, which includes the network, servers, storage, and operating systems. Strong authentication, access control, logging and auditing, and other critical functions must also be implemented for the *ESS components.* Furthermore, vulnerability management and patching must be consistently implemented for all systems. Without it, each site will independently operate with deprecated operating systems, unpatched vulnerable applications, and unmaintained security software releases no longer supported by the manufacturers. Implementation of all such system management and continuous monitoring functions requires in-depth vendor- and product-specific expertise and configuration planning for the ESS headend applications, field panels, and other elements of the system.

Extensive Integration Requirements

Electronic Security Systems are increasingly composed of multiple elements and require integration with a range of applications and enterprise services. Here are some of the examples of ESS capabilities and compliance needs that drive integration requirements:

1. **Cardholder Replication:** Enrolled CACs and PIVs are distributed to all enterprise PACS so that personnel can easily obtain facility access.
2. **Remote Alarm Monitoring:** The Government can perform regional and central alarm monitoring and ensure security force responses are compliant with policies.
3. **Access Management:** Manage access privileges for existing personnel and badge holders.
4. **Visitor Management:** Sponsor visits, perform background checks on visitors, manage visitor arrival, provision and deprovision security access, and perform audit logging of all access.
5. **Information Assurance Logging and Auditing:** Audit privileged PACS users and ensure only authorized changes are performed.
6. **Integrated Security:** Centrally manage integrated intrusion detection, closed-circuit television (CCTV), and access control for interior and exterior spaces.
7. **Integrated Computer Aided Dispatch:** Securely deliver alarms and event notifications to computer-aided design (CAD) systems and mobile devices.

Recommendations

To address the challenges identified in this white paper and to effectively employ emerging system capabilities, the electronic security leadership may consider the recommendations outlined below.

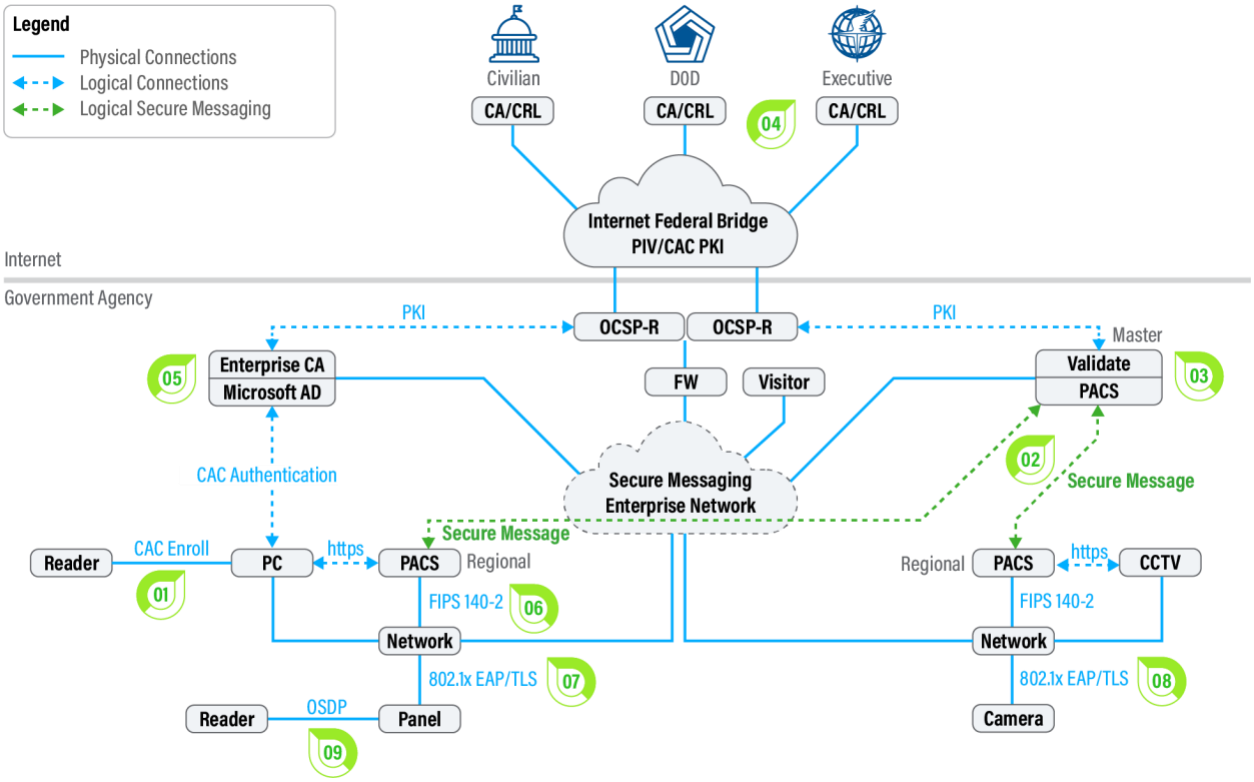
Recommendation 1: Reference Architecture for Enterprise ESS Deployments

Establish a reference architecture for enterprise electronic security systems consistent with FIPS 201, FICAM, NIST 800-116, NIST 800-53 and related standards to provide the foundation and consistent implementation of the following:

- The federated nature of enterprise-wide security systems
- Multi-tier operational model
- Integration with enterprise network and services
- Secure internet connectivity to enable PKI interoperability and connectivity to the Federal Bridge
- PKI-based authentication of ESS components

Figure 2 illustrates how PKI and Enterprise certificates are used within a typical FICAM PACS for secure authentication, encryption, and validation, which must be incorporated in the reference architecture.

FIGURE 1: PKI AND ENTERPRISE CERTIFICATE OPERATION WITH FICAM PACS



	Definition		Definition
01	Create or enroll CAC certs into Microsoft AD, PACS, and CA.	06	PACS communicates to electronic panels via FIPS 140-2 encryption using enterprise client certs
02	Replicate CAC certs throughout enterprise using secure messaging via client-server certs from PACS to PACS Master and enroll into PKI validation.	07	Electronic panels network authenticate via 802.1x using EAP/TLS client certs and download all CAC certificates from PACS

03	Replicated CACs are enrolled into PKI validation server and validated on an 18 hour basis.	08	Cameras stream using https client-server certs and 802.1x authenticate to FIPS 201 readers
04	Enrolled CAC certs are validated via OSCP-R against Federal Bridge CA and revoked certs invalidated.	09	CAC cards authenticate to FIPS 201 readers using multi-factor PIV of OSDP
05	Issue enterprise certs to servers, desktop PC's, and devices for secure machine to machine communications.		

Recommendation 2: ESS Enterprise Network and Core Services

To support the ESS reference architecture, ESS leadership should consider and take steps towards developing a consistent ESS enterprise network enclave implementation approach. To maximize efficiency, security, and flexibility, the approach should include the following:

- **Maximizing the use of existing accredited networks**. To avoid excessive costs while maximizing security benefits and capability reuse, the ESS enterprise network enclave may rely on the existing Non-secure Internet Protocol Router (NIPR) networks as the underlying transport and the Internet Protocol Security (IPSec) Virtual Private Network (VPN) technology to achieve cryptographic isolation.
- **MS Windows domain services**. Microsoft Windows domain services to allow for effective use of group policy objects and other capabilities to meet the system hardening requirements in accordance with DOD Security Technical Implementation Guides (STIGs).
- **Secure Internet Connectivity.** The ESS enterprise network architecture must provide for secure internet connectivity via a firewall-controlled connection to the underlying authorized network (NIPR) to enable access to Federal Bridge and participating Certificate Authorities, and to enable interoperability for federal PKI credentials.
- **Enterprise Certificate Authority (Enterprise CA)** to support authentication of ESS devices and components.
- **Access to system management and continuous monitoring services**. Vulnerability Management, configuration, patch management, boundary protection, host-based security, security information and event management (SIEM), and other critical continuous monitoring services must be deployed on the enterprise ESS enclave or accessible via a secure, firewall controlled, connection to the underlying authorized network (NIPR).

Recommendation 3: Open Architecture for Enterprise Integrations

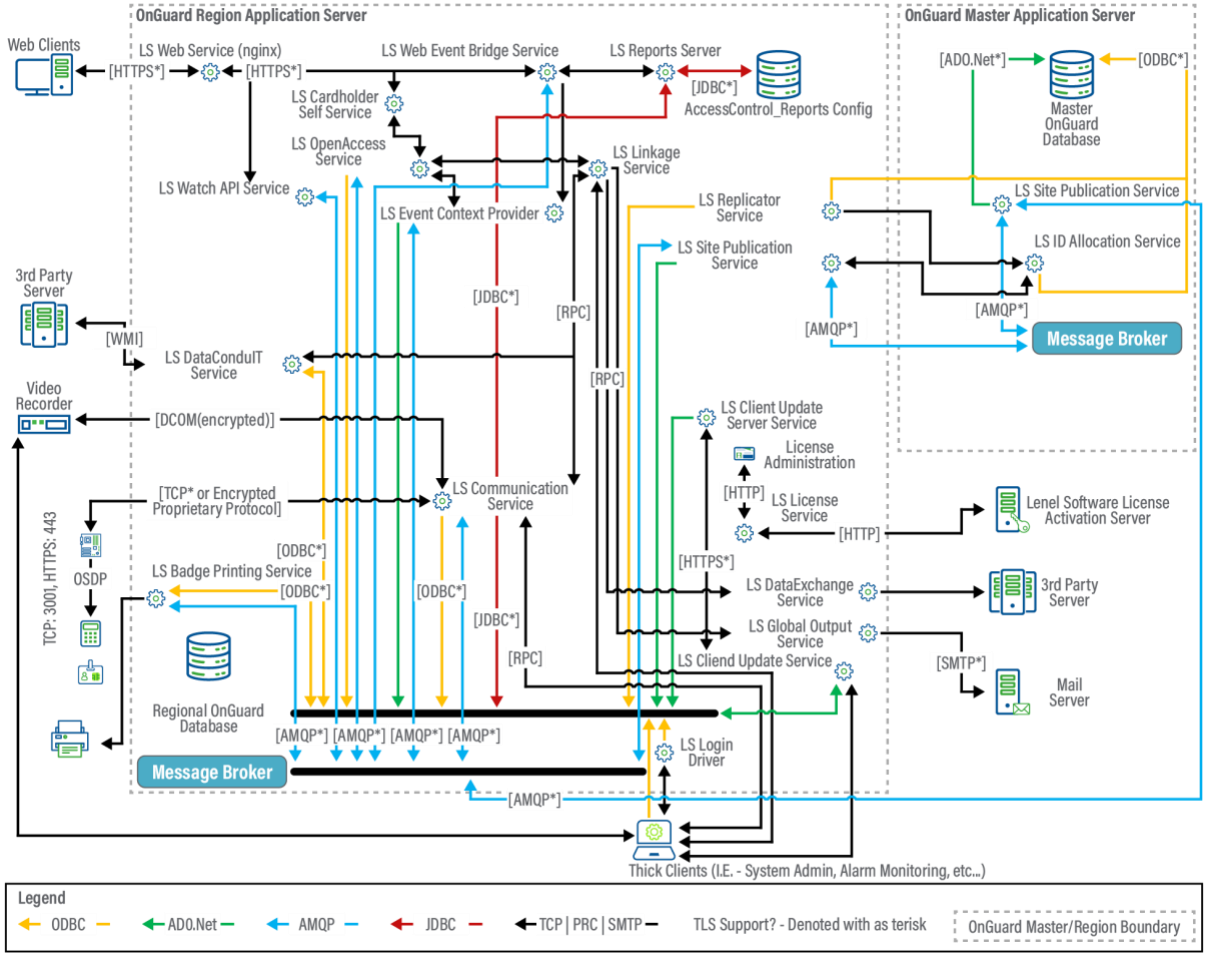
To provide for scalability and maintainability of a distributed ESS, the ESS leadership needs to develop a robust application integration approach, which supports the increasing number of use cases, such as the ones identified in the "Extensive Integration Requirements" section above. While proprietary, PACS-specific integration/messaging architectures work well within a homogeneous PACS architecture, the approach may not scale to the enterprise-wide deployment. When developing the integration approach, the ESS leadership should consider multiple factors, including but not limited to the following:

- **Security**. The integration approach should integrate security mechanisms, such as encryption and strong authentication between publishers, subscribers, and message brokers to protect the communication that may otherwise be exploited to unsecure spaces, unlock doors, and identify security coverage gaps.
- **Version-independent data model**. Vendor-specific, proprietary integration interfaces often require every PACS system, workstations, and panels to be upgraded simultaneously when the system version changes. Depending on the size of the enterprise, this upgrade can result in a long maintenance window that significantly impacts security operations. An open architecture approach should provide an application programming interface (API), which is largely independent of the PACS version and allows for enterprise operation with endpoints running different versions of software.

- **Multi-vendor integration**. To support integration with visitor management systems, provide for enterprise-wide cardholder database replication, allow for integration with SIEM platforms to implement auditing and accountability controls, and to facilitative integrated security management functions (access control, intrusion detection, CCTV, etc.), the integration approach should ideally rely on open source or commercially available technologies, such as RabbitMQ, NiFi, and ApacheMQ. The use of such technologies decouples the integration/enterprise messaging architecture from a single security application.

Below is an example of a data flow diagram for a common PACS system by Lenel, outlining all of the different secure communications between Enterprise applications and services. The Advanced Message Queuing Protocol (AMQP) sends messages securely between systems via a Message Broker. The AMQP messages, that contain sensitive system status and control information, utilize Enterprise certificates to ensure that all security-related messages are accessible only via trusted publishers and subscribers. While this diagram deals with a single specific PACS flavor, it illustrates both the complexity and crucial importance of developing a sound application integration approach.

FIGURE 2: CRITICAL INTEGRATION INTERFACES WITHIN THE LENEL ONGUARD® SYSTEM ARCHITECTURE



Recommendation 4: Enterprise Technical Standards and Technical Guides

The effectiveness of the enterprise security system and the security of the protected physical and IT asset depend on reliable requirements capture and consistent design, implementation, and operation of ESS.

To manage the growing complexity and diversity of ESS implementations and the critical interfaces to the underlying IT infrastructure and to critical external services, ESS leadership should look to develop, implement, and enforce a set of standards, including but not limited to the following:

- **Enterprise-Wide Model-Based Design Standards and Practices**. To ensure consistent application of the technical configuration guides and to enable industrialized, modular delivery methods, the enterprise should consider employing and integrating data-centric design practices, such as building information modeling (BIM) and model-based systems engineering (MBSE). Using these practices and associated tools, the DOD enterprise can "codify" the use of proven and repeatable system architecture and design elements.
- **Technology-specific implementation guides**. Similar to the DISA STIGs that ensure consistent hardening of IT components, the DOD ESS leadership should develop platform- and product-specific technical implementation and administration guidelines to ensure consistent configuration, operation, and maintenance of the various ESS components. Critically, such guidelines should go beyond the IT-centric parameters (covered by the DISA STIGs) and focus on the effective ESS configuration and use of features, functionality, and device programming relevant to security operations, e.g. access control templates, IDS templates, CCTV integration, event customization, alarm prioritization, user roles and privilege levels, etc., as well as integration with enterprise services, such as SIEM.

Conclusion

Due to their transformation from local facility functions to IT-enabled enterprise systems, successful deployment and operation of modern ESS depends on effective **systems engineering** functions that include:

- System architecture leadership: development of the reference architecture and system performance standards
- Capability planning: development of the concept of operations and operational interfaces to be enabled by the system and formulation of the functional and performance requirements for each deployment
- Design: system functional design, installation design, and development of testing procedures and acceptance criteria
- Implementation: System integration, configuration, programming, and commissioning, inclusive of the cybersecurity functions, such as applying security technical implementation guides
- Operation and maintenance of the ESS, as well as performing cybersecurity maintenance and continuous monitoring functions (e.g. weekly patching of all operating systems and applications, scanning for vulnerabilities and information assurance (IA) compliance, and performing technology refreshes and new application releases)

To be successful, these enterprise functions must combine and fundamental system engineering approach with ESS and information technology expertise supported by a combination of specialized tools and methods, such as model-based systems engineering.

Appendix

Glossary of Terms

Acronym	Terminology
IT	Information Technology
ESS	Electronic Security Systems
NIST	National Institute Of Standards And Technology
PACS	Physical Access Control Systems
ATO	Authorization To Operate
ICD	Intelligence Community Directive
DOD	Department Of Defense
FISMA	Federal Information Security Management Act
FIPS	Federal Information Processing Standards
PKI	Public Key Infrastructure
FICAM	Federal Identity Credentialing And Access Management
CHUID	Card Holder Unique Identifier
ePACS	Electronic Physical Access Control Systems
CAC	Common Access Cards
SCIF	Sensitive Compartmented Information Facility
EOC	Enterprise Operations Center
CAD	Computer-Aided Design
NIPR	Non-Secure Internet Protocol Router
IPSec	Internet Protocol Security
VPN	Virtual Private Network
STIG	Security Technical Implementation Guide
Enterprise CA	Enterprise Certificate Authority
SIEM	Security Information And Event Management
API	Application Programming Interface
AMQP	Advanced Message Queuing Protocol
BIM	Building Information Modeling
MBSE	Model-Based Systems Engineering
IA	Information Assurance