REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
31-10-2016	FINAL	Mar 2015 – Mar 2016

4. TITLE AND SUBTITLE

The case for using DBIDS to control Physical Access Control systems and the justification to certify DBIDS and IMESA for the Enterprise networks and DoD cloud

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

CDR Robert Hanvey, USN

Paper Advisors: **Dr. William Bundy and Mr. Walter Bonilla**

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Gravely Naval Research Group
U.S. Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited. Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES

14. ABSTRACT

A fundamental shift has occurred over the last 10 years in how access control is viewed and the identity is the focus not physical barriers to entry. With the Homeland Security Presidential Directive-12 (HSPD-12) requirement for a common Federal identification, the Federal Information Processing Standard (FIPS 201) technical specification of the same, coupled with the ensuing verification and authenticating measures that must be met before granting access, the battle is nearly lost. The Federal Government and the DoD have lost the capability for a single watch stander at a door or gate to properly evaluate if the person asking for access meets all criteria without technological assistance. The Physical Access Control Systems (PACS) at DoD base main gates and into every building which access must be controlled are run via a patchwork of commercial off the shelf (COTS) software solutions. The DBIDS platform needs to be tested for, and given any missing functionality required, to manage and run the PACS currently run by COTS software at all DoD locations. In addition, both the DBIDS and IMESA platforms must be certified for use on the Enterprise networks and eventual migration to the DoD cloud in order to maintain the future security of the PACS and to keep pace with the inevitable changes in technology.

15. SUBJECT TERMS
Physical Access Control Systems DBIDS IMESA PACS Cloud Enterprise Networks

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Dr. William F. Bundy, Director Gravely Naval Research Group
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	UNCLASSIFIED	**23**	**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			401-841-2674

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

The case for using DBIDS to control Physical Access Control systems and the justification to certify DBIDS and IMESA for the Enterprise networks and DoD cloud

by

Robert Hanvey

CDR, USN

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____//S//_____

31 Oct 2016

ABSTRACT

A fundamental shift has occurred over the last 10 years in how access control is viewed and the identity is the focus not physical barriers to entry. With the Homeland Security Presidential Directive-12 (HSPD-12) requirement for a common Federal identification, the Federal Information Processing Standard (FIPS 201) technical specification of the same, coupled with the ensuing verification and authenticating measures that must be met before granting access, the battle is nearly lost. The Federal Government and the DoD have lost the capability for a single watch stander at a door or gate to properly evaluate if the person asking for access meets all criteria without technological assistance. The Physical Access Control Systems (PACS) at DoD base main gates and into every building which access must be controlled are run via a patchwork of commercial off the shelf commercial off the shelf (COTS) software solutions. The DBIDS platform needs to be tested for, and given any missing functionality required, to manage and run the PACS currently run by COTS software at all DoD locations. In addition, both the DBIDS and IMESA platforms must be certified for use on the Enterprise networks and eventual migration to the DoD cloud in order to maintain the future security of the PACS and to keep pace with the inevitable changes in technology.

Contents

LIST OF FIGURES

INTRODUCTION

> This all comes back to the Washington Navy Yard process, which was a big deal -- but the real change that happened was the physical security community and the IT guys talked to each other and said, 'You know what, it's not a physical security problem; it's an identity problem,..[1]

The change referenced above by Michael Butler, Deputy Director for Identity Services at the Defense Manpower Data Center, illustrated the ongoing paradigm shift in viewing access control requirements for Defense facilities. Access control is no longer barbed wire, heavy gates and gun toting security. Access control now focuses on properly identifying who is requesting access and if they have the required fitness to gain entrance.[2] This shift, along with the near full implementation of the Department of Defense (DoD) statutorily required access control measures highlights the need to maintain focus on standardizing not only the physical technology, but the software platforms and connectivity for these Physical Access Control Systems (PACS). With potentially a long and complicated path for certification to operate software on the Enterprise networks, current DoD PACS solutions are instead connected via local workstations which access the required databases for verification and vetting through commercially procured Internet Service Providers or service specific non-enterprise networks. For example, to compensate for the differences in systems and PACS software, The Navy and the Naval Reserve have made great strides in

[1]Sternstien, Alyia. "Getting on Military bases is about to involve FBI background checks" His comments were at a Smart Card alliance event in July, 2014. Nextgov.com, 04 Aug 2014. www.nextgov.com/defense/2014/08/getting-military-bases-about-involve-fbi-background-checks/90431/ (accessed 30 Oct 2016).

[2] "fitness" to gain access is defined by several factors to include proper identity proofing and vetting, that they possess a credential authorized to access the facility and the individual matches the presented credential.

identifying and implementing standardized PACS solutions across varied commands to mitigate these effects but still operate with a patchwork of commercial off the shelf (COTS) software platforms. Those accomplishments are in danger of evaporating if a long-term solution of complete integration with the enterprise networks and eventual migration to the DoD cloud does not happen.

BACKGROUND

The big change in access control requirements is most often traced back to August, 2004, with the publication of Homeland Security Presidential Directive-12, commonly referred to as HSPD-12. In this memorandum, President George W. Bush identified a gap in security through the "wide variations in quality and security of forms of Identification used to gain access to secure Federal and other facilities…"[3] He outlined the threat from terrorist activities through these gaps and created the policy for a "...mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors, (including contractor employees)."[4] This common Identification was to be utilized for "physical access to Federally controlled facilities and logical access to Federally controlled information systems"[5] The intent was a common identification which to standardize access controls and leverage the purchasing power of the Federal government to reduce costs while improving security. HSPD-12 further directed the Department of Commerce to publish those specification guidelines.

[3] Homeland Security Presidential Directive-12, 27 Aug 2004. Paragraph 1. https://www.dhs.gov/homeland-security-presidential-directive-12
[4] Ibid. HSPD-12. Paragraph 1.
[5] Ibid HSPD-12 Paragraph 4.

HSPD-12 guidelines were captured in Federal Information Processing Standard (FIPS) publication number 201, or herein referred to as FIPS 201. First published in February 2005, FIPS 201 established the standard which "specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors."[6] FIPS 201 captures the requirements and specifications of a Personal Identity Verification (PIV) card required to meet the HSPD-12 directive. The DoD commonly referes to their PIV compliant card as the Common Access Card or CAC. Most references in this paper will be to a PIV compliant card which includes the DoD CAC. A key component of the FIPS 201 standard is the technical interoperability with various federal Departments and Agencies.[7] It is through this interoperability that a single identity credential can be used to verify several levels of credentialing and authentication across multiple Federal departments and agencies. This laid the groundwork for stronger authentication measures and expansion of use for access control beyond visual authentication or local technological solutions.

While the PIV compliant cards were in use, they had limitations in employment which would require planning and better defined interoperability standards. In November 2008, the National Institute of Standards and Technology published Special Publication 800-116, A Recommendation for the use of PIV credentials in Physical Access Control Systems (PACS).[8] This publication identified the use of widely varied solutions in PACS technologies through the Federal government and called for a common PACS standard in which the technological characteristics of the PIV cards could be leveraged and possibly expanded. While the FIPS 201 standards defined the technological requirements of how PIV

[6] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
[7] Abstract, page iii http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
[8] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-116.pdf

cards would be authenticated, it did not outline any uses or applications for the same.[9] These capabilities were not utilized for PACS as the standards were not written to meet the widely varied solutions across the force.

With local PACS technological solutions, security was often assumed to be higher. This was thought to be because the lack of published standards or plans meant it was difficult for an outsider to know how that system operated and where it was vulnerable. However the ease of counterfeiting or cloning the local PACS ID cards showed the PACS was not as secure and was exposed to a higher overall security risk. This extra risk was due to questionable authentication assurance which lowered overall security assurance.[10] In addition, local solutions typically lacked interoperability with other Federal systems. This was a natural result from only purchasing PACS to meet local requirements instead of a combined approach which includes future requirements and interoperability. The lack of interoperability and ability to authenticate credentials with a high degree of assurance meant access control to federal facilities were vulnerable to unauthorized entry as promulgated in HSPD-12. NIST 800-116 outlined these technical and security roadblocks and recommended a number of technical solutions and minor changes to the FIPS 201 to standardize methods of access control that could be utilized with the PIV compliant cards. These measures were designed to address the security shortcomings which resulted from the lack of a standardized PACS implementation. However, these measures could not be implemented until a majority of the Federal employees were in possession of a FIPS 201 compliant PIV card. By 2011, this milestone was met when 5 million of 5.7 million current federal employees and

[9] Ibid. NIST 800-116 2.2 Background
[10] Ibid. NIST 800-116

contractors had undergone the required background investigations and 4.5 million had HSPD-12 compliant PIV credentials.[11]

With a majority of the Federal employees credentialed, White House memorandum M-11-11, signed Feb 2011, directed an accelerated push to utilize the electronic capabilities of the PIV credentials to include many of the NIST 800-116 recommendations. The Department of Homeland Security (DHS) memorandum attached to the M-11-11 memo dictated that an Agency's policy includes the following requirement: "Agency processes must accept and electronically verify PIV credentials issued by other federal agencies".[12] The ability to electronically verify PIV credentials ensured the intent of HSPD-12 interoperability was met. This meant the various Federal agencies access control systems must have the ability to electronically verify not only that the PIV card through the FIPS 201 standards, but those credentials were verified against the proper federal database within a required timeframe of the attempted access request. Specifically, the PIV certificate presented must be verified as valid at the time of registration and ensured that the issuing certificate authority did not place the certificate on the certificate revocation list (CRL). The CRL verification also had a time restriction; that the database information utilized was required to be current within the 6 hours of the PIV card enrollment.[13] Both these capabilities require connectivity between the PACS and the databases as well as periodic monitoring to identify any change in eligibility status of the PIV card holder. This capability is at the core of the e-verify requirement as well as the required criminal background vetting.

DEPARTMENT OF DEFENSE REQUIREMENTS

[11] White House Memorandum M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors. Feb 03 2011. http://www.cac.mil/docs/m-11-11.pdf (29 Oct 2016).
[12] Ibid. White House Memo M-11-11.
[13] PKI in E-PACS Procurement Guidance. Version 1.1.0 Office of Technology Strategy, Identity Management Division. Washington D.C. 24 February 2015.

With the enactment of the National Defense Authorization Act (NDAA) for Fiscal Year 2008 (FY08), section 1069 of that law contained statutory guidance for DoD access standards with achievement milestones for implementation. Section 1069 directed the Secretary of Defense to develop access standards applicable to all military installations in the United States by January 1, 2009.[14] While subsequent NDAAs extended the required implementation date by 2 years, the requirement remained to develop the standards for access, screening requirements to include protocols, standards and methods for verifying both the fitness and identity of the individual requiring access. On December 8th, 2009, the Secretary of Defense issued Directive-Type Memorandum (DTM) 09-012 to implement the section 1069 requirements.[15]

ELECTRONIC VERIFICATION AND VETTING

DTM 09-012 outlines how the access requirements listed above will be implemented in PACS and defines their required interoperability. Section 3 (2) establishes the requirement that, "… PACS must support a DoD-wide and federally interoperable access control capability that can authenticate USG physical access credentials and support access enrollment, authorization processes, and securely share information."[16] The requirement to securely share information and maintain federal interoperability set new thresholds for the PACS they could not meet for several years because the capability was only in the research stages. These requirements would later be met with the Defense Biometric Identification System (DBIDS) platform. In addition to defining access vetting and authentication for PIV

[14] *National Defense Authorization Act for Fiscal Year 2008*, H.R. 4986, Public Law 181, 110th Congress, January 28th 2008.
[15] Department of Defense. Directive-Type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access .
[16] Ibid DTM 09-012.

or DoD-issued card holders, DTM 09-012 outlined requirements for those requesting access who presented non-Federal Government and non-DoD-issued identification. The vetting of the claimed identity of those personnel as well as their fitness to gain access would be evaluated through the FBI crime database, specifically via the National Crime Information Center (NCIC) as well as the Terrorist Screening Database (TSDB).

CRIMINAL BACKGROUND CHECKS

The NCIC database access presents some unusual problems as there are legal limits limiting who can query the database and how its data can be shared. NCIC data contains sensitive law enforcement information and access is restricted to Law Enforcement (LE) only. Initially, manually entering data into a NCIC terminal was the only method for the DoD to check an individual was in the Wanted Persons Files.[17] The information returned from the NCIC database would indicate if LE had an interest in that individual and access should not be granted unless escorted. This is an acceptable method for full background checks to gain access to controlled or restricted areas or where time is not critical and consistent and repeated access would require a local badge. On the other hand, the NCIC terminal is not a viable solution for vetting all or even a small percentage of random traffic stops to keep the lines moving. In addition, a majority of those performing the visual vetting for access control at base main gates are not LE, but regular military personnel watch standers that went through local training. These non-LE gate guards are not legally authorized to view the data of the NCIC database for an individual in question. That is the

[17] NCIC accesses the FBI databases for police and law enforcement "wants" and "warrants". The Wanted Persons files contain individuals who may have arrest warrants, be on the lookout (BOLO) warnings, and other histories of criminal behaviors or charges.

crux of the need for a platform to interface the LE restricted databases and output sanitized data for use in vetting fitness to be granted access.

A SOFTWARE PLATFORM TO INTEGRATE ALL REQUIREMENTS.

A single cross-domain platform capable of interfacing the varied databases to include restricted ones such as NCIC, had been under development for several years. The Defense Installation Access Control (DIAC) Working Group had a platform in development, called Identity Matching Engine for Security and Analysis (IMESA). IMESA could query NCIC and the TSDB as well as all the required databases such as DEERS for access vetting and authorization.[18] And most important, IMESA can identify and report derogatory LE information without requiring LE interface. With these capabilities fully tested and implemented, IMESA became the platform utilized to meet the requirements laid out in DTM 09-012. This created a "one-stop-shop" platform that could interface with all required databases and relay sanitized information to the personnel performing the vetting. The IMESA output could be programmed in various manners to categorize authorization approval level. One common method is using colors such as green/yellow/red to show the non-LE security guard confidence level of the ability to grant the access request.

Figure (1) & (2) below show a security guard's scanning a PIV/CAC card and the scanner screen output with the color green at the bottom, indicating the ID presented passed authentication. Assuming no other concerns were present, access could be granted. Yellow would indicate caution must be used before granting any access until more information is gathered and an informed decision can be made. Red would indicate access is not authorized

[18] *Identity Matching Engine for Security Analysis, (IMESA)* Defense Manpower Data Center (DMDC) info brief. https://dbids.dmdc.mil/DUG/2016/day-two/06-IMESA.pdf (accessed 30 Oct 2016).

unless they are escorted and comply with any restrictions the base commander or appropriate authority has established for escorted access.

Figure 1 Image of hand scanner scanning PIV card. [19]

Figure 2 Screen-shot showing individual is authenticated and authorized access with a "Green" indication status.[20]

[19] Samantha Jones, U.S. Navy photo. http://jaxairnews.jacksonville.com/2014-09-03/notice-id-scanning-effect-all-gates (accessed 31 Oct 2016).
[20] Frank H. Carter, U.S. Air Force photo. http://www.sheppard.af.mil/News/Photos.aspx?igphoto=2000147223 (accessed 31 Oct 2016).

IMESA is a critical piece of the security and force protection as it enables non-LE personnel to perform mandated access screening in high traffic areas such as main gate entries. It accomplishes this while ensuring Personally Identifiable Information (PII) information is contained and criminal concerns discovered through NCIC remain only visible to a Law Enforcement Officer (LEO). This fully meets the requirements laid out in DTM 09-012. But at the time DTM 09-012 was published, there were several roadblocks preventing full implementation, the least of which was lack of a developed software platform to execute the checks, (IMESA).

This policy, (DTM 09-012), could not be implemented until the DoD established a policy authorizing IMESA access other federal agency databases such as the FBI. It was not until May 2014 when the DoD issued DTM 14-005, establishing the policy for accessing the Federal Bureau of Investigation (FBI) NCIC files via IMESA. Figure (3) below shows the process and how each part interacts. IMESA was first implemented in August, 2014 in several locations. As of August, 2016, 274 sites were outfitted with 16 more scheduled to go live through the December, 2016. This widespread implementation has allowed IMESA to identify over 6 million ID card credentialing issues along with 11,000 alerts from NCIC via IMESA when personnel presented an ID for access permission. In addition, 3400 had active ID credentials when IMESA identified felony warrants out for their arrest when they attempted to obtain permission for access. These flagged personnel, along with those in Figures 4-6, show the positive impact IMESA has on keeping our facilities and bases safe and secure with only 2 years and very small numbers of access points utilizing IMESA until recently.

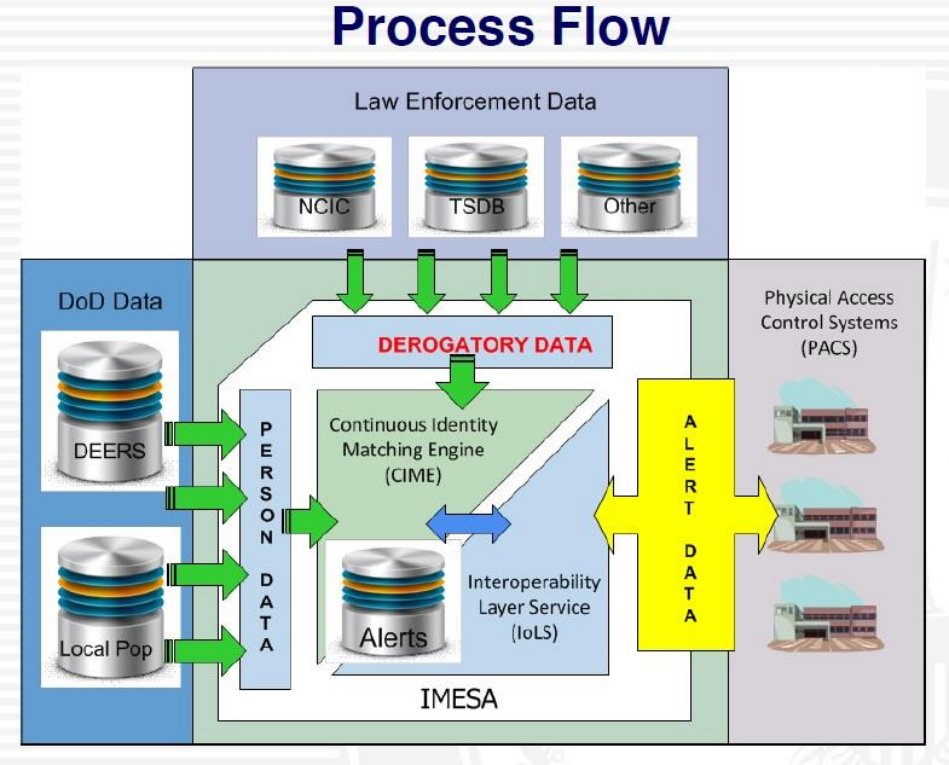

Figure 3 The process flow of IMESA integrating with the various databases both restricted and not restricted.[21]

All-Time Person-Alert Matches

2 August 2016

PACS	NCIC Alerts	PACS Alerts	Total
DBIDS	9,508	13,237	22,745
AIE	1,477	722	2,199
Enabler	51	94	145
Total	11,036	14,053	25,089

Figure 4 All time NCIC alerts since roll-out in 2014.[22]

[21] DMDC DBIDS website. August 2016 IMESA statistics briefing. http://dbids.dmdc.mil/resources.html (03 Nov 2016).
[22] Ibid.

All-Time Card Revocations

2 August 2016

PACS	Lost/Stolen DoD Credentials *	Terminated DoD Credentials	Lost/Stolen PACS Credentials	Terminated PACS Credentials	Total
DBIDS	2,099,570	2,680,756	990	82,297	4,863,613
AIE	596,070	595,934	4	397	1,192,405
Enabler	33,515	35,584	10	34	69,143
Total	2,729,155	3,312,274	1,004	82,728	6,125,161

* Lost/Stolen DoD Credentials – The earliest record was reported in 2004 inside the IMESA database.

Figure (5) Total number of times a presented ID card was denied access because it was on the Certificate Revocation List, was listed as stolen, terminated/expired or the member was no longer eligible for the card. Does include incidents before roll-out with IMESA in 2014. However, enrolled population was much smaller than the ~6 million actively enrolled personnel in Aug of 2016. Reasonable to assume a majority of these numbers are since 2014 when the database size increased substantially. [23]

IMESA Subset of Active NCIC Alert Matches

*Category	August 2016
Assault	906
Desertion	413
Murder	85
Sex Assault	336
Kidnapping	76
Robbery	134
Burglary	401
Dangerous Drugs	626
Sex Offense	267
Weapons Offense	157
Total	3,401

*Person had an active credential at the time of warrant

** This is cumulative data showing match quantities for egregious crimes.

Figure (6) Numbers of denied access because IMESA found a Felony Want or Warrant on the individual and denied their access request the next time they attempted to enter the base or facility.[24]

[23] Ibid.
[24] Ibid.

MOVING FORWARD WITH COMMON SOLUTION

IMESA meets two key requirements for the way forward on single common system PACS for all DoD facilities. First, it enables access to mandated vetting databases with the ability to sanitize the data as needed for non-LE security guards. Second, IMESA, coupled with Defense Biometric Identification Data System (DBIDS), will standardize access control across the DoD and offer growth capacity while maintaining the required interoperability vs. shortfalls with individual site PACS. IMESA and DBIDS are in a constant state of updates and expansion of capabilities. The most recent capability added to IMESA was the connection to the National Sex Offender Registry (NSOR) in accordance with DTM 15-003.[25] Critically, the ability to continuously monitor all registered personnel and update any number of the current databases queried ensures IMESA will remain a relevant and capable platform for years and will provide the appropriate base for eventual transition of all software solutions to the cloud and connectivity already provided for all enterprise workstations.

IMESA is a prime example of how an enterprise-wide solutions can outperform multiple individual and service specific solutions. While it appears IMESA answers the PACS challenges of vetting, it only addresses the database queries portion. We still require software platforms to run the PACS and certify and authorize access while processing the various levels of authentication from PIV cards, fingerprints, contactless readers and eventually, other biometric readers such as iris readers.

DEFENSE BIOMETRIC INFORMATION DATA SYSTEM (DBIDS)

DBIDS was conceived in 1995 to protect the Combined, (USAF – Republic of Korea (ROK)) Command Center in the Republic of Korea. Starting as a joint project across several

[25] http://www.dtic.mil/whs/directives/corres/pdf/DTM15003.pdf

United States (U.S.) agencies, mostly DoD, it achieved full implementation when Force Protection Condition Delta was directed for all U.S. Forces Korea (USFK) in September, 2001.[26] Primarily conceived an overseas capability, over the next 7 years, DBIDS was deployed at locations in the Asia and Middle East, with a single CONUS stand-alone location at Fort Hood. With concerns about attacks on CONUS bases, NORTHCOM requested deployment of the system to 13 CONUS Air Force bases in 2007/2008.[27] NORTHCOM then took DBIDS through some testing to prove the concept and find a way to implement DBIDS with all DoD forces, not just at overseas locations. With several false starts in the attempts to fully implement DBIDS across the DoD, it gained substantial traction when the Defense Installation Access Control Working Group was formed in early 2009. The DIAC Working Group was formed from representatives of all the DoD services and agencies with the goal to build a roadmap for implementation while working out the bugs.

A second set of tests were done in 2010/2011 leading into mature testing and further development over the next 2-3 years. The Air Force received some of the first DBIDS systems with new capabilities. The other services have followed suit with system deployment and implementation as budgets allow. An important point is the capabilities of the current DBIDS systems coupled with the IMESA platform are orders of magnitude more capable than the DBIDS systems commands utilized over the 2001-2013 timeframe.

THE ENTERPRISE SOLUTION (RECOMMENDATIONS)

With DBIDS controlling the access control systems but utilized primarily for hand-held scanners at perimeter checkpoints and IMESA providing standardized and expandable

[26] http://www.reginfo.gov/public/do/DownloadDocument?objectID=9723501
[27] Ibid.

database vetting and integration, only two issues remain in the way of implementing a common DoD Enterprise-level solution. DBIDS scanners at base main gates are a common sight for a majority of the DoD and are approaching full integration but not yet utilizing the full capabilities of the platform. The first shortfall is the need to research and develop the DBIDS capability to run PACS not only at a main external gate for ID card vetting, but at the doors of every building or location which requires a PACS. The second issue is submitting the PACS for testing and approval so they can be certified for use on the enterprise workstations utilizing the enterprise connectivity. This removes the need to purchase a separate commercial T1 for each building or expanding a network like the Navy's PS net to connect all these PACS.

Today DBIDS is utilized primarily via the hand held scanners to integrate IMESA capability into screening. DBIDS is an enterprise-wide software ***ACCESS CONTROL*** system that is used more for ID and background vetting than electronic control/integration with the physical locks and control circuits of the buildings with PACS. Some Marine commands have started some informal testing using DBIDS to control building PACS to include control of the contactless readers and locks for the controlled entries.[28] The enormous benefit of this approach is in the saved expenditures on access control and registration software, non-enterprise workstations or servers and upgrade costs each time the commercial software company makes a change or goes out of business.

Leveraging the immense capability of DBIDS and adding what minimal extra capability may be required to interface with the building PACS will have an outsized return on the investment. Current strategy has the DoD purchasing different COTS solutions for each location and in some cases, each building on the same base. These PACS workstations

[28] John Salley, email conversation 03 Nov 2016.

are not authorized to access internet connectivity via the local NMCI or appropriate Enterprise DISA circuits. With the DoD moving aggressively to shift all current storage and software to the cloud over the next few years, now is the time to work approval for DBIDS to operate on the Enterprise workstation and eventually in the enterprise cloud.

CONCLUSION

The DoD is at a decision point much like the U.S. was upon implementation of the common ID card mandated by HSPD-12, the White House Memorandum M-11-11 accelerating implementation and leveraging the technological opportunities contained in the FIPS 201 standard for PIV cards, and DTM 09-012, which solidified the DoD requirement to electronically verify and perform a criminal background check on all requesting access to DoD facilities. Those three milestones drove development of IMESA and DBIDS to the presently capable, yet expandable, interoperability platforms they are today. With the relatively rapid deployment of PACS in buildings DoD wide, the robust capabilities of IMESA and DBIDS to work with these existing hardware and controls must be leveraged to minimize cost down the road and loss of capability requiring an entire new PACS yet again. DBIDS is a very flexible platform which likely can be adapted to work with many different make and models of PACS as the controls for doors are typically very similar between manufactures. In addition, the PACS already must comply with the FIPS 201 standards, (or they would be new systems if they couldn't). Looking ahead, the lead time for software approval for enterprise computers and networks can be very slow, so now is the time to begin

that process to understand what must change to comply with IL-4 and IL-5 cloud security requirements.[29]

The need to expand and adapt the platforms will be required independent of any decision to move the software into the enterprise cloud. In 10-15 years, the access control systems MUST be behind the firewall and security of the DoD cloud in order to protect increasingly technological weapons systems, knowledge and capabilities. If the PACS are left outside of the enterprise network solution, they will forever be limited in ultimate security and capability if the expectation is consistent protection force-wide.

One nearly certain change in the next 5 years is the shift away from the Common Access Card (CAC/PIV compliant) as the sole method for vetting and access at even the most basic levels. The CAC won't be completely eliminated, but the plan is already underway to discontinue use for "logical" access by mid-late 2018.[30] The DoD Chief Information Officer, Terry Halvorsen, told a audience at the 2016 Federal Forum in July of this year, that "We are embarking on a two-year plan to eliminate CAC cards from our information systems…We may still use them to get in the building, but we're not going to use them on our information systems."[31] In the same speech, he emphasized the push away from single factor authentication for system access and a shift to biometric and true multifactor authentication.[32] The good news with this rapid shift in both the authentication factors and the upcoming move to the cloud is a majority of existing PACS meet FIPS 201

---

[29] The transition to the DoD cloud is different in a number of respects to traditional software installed on a workstation. The DoD Cloud Computing Security Requirements Guide is linked at the end of this footnote. It is a 150 page document covering all aspects. http://iase.disa.mil/cloud_security/Documents/u-cloud_computing_srg_v1r1_final.pdf (03 Nov 2016). A non-governmental advisory group has a number of resources they prepared to address the shift to the cloud for the DoD. While some information may be biased in one way or another, the overall products are worth a review to help understand the challenges and requirements of the transition. http://www.cloudcomputingcaucus.org/recent-research/ (03 Nov 2016).

[30] "Logical" access is access to IT systems where

[31] Sean Waterman *DOD plans to eliminate CAC login within 2 years.* Fedscoop.com article. 14 June 2016. (accessed 30 Oct 2016).

[32] Ibid.

compliance and interoperability already. Therefore, adding a fingerprint or iris scanner to increase the authentication factor and confidence will be straight-forward and dovetails with an effort to move the entire platforms to the cloud.