# Continuous Monitoring of Cybersecurity in a Training System Environment

**Graham Fleener**
**U.S. Army PEO STRI**
**Orlando, FL**
**graham.g.fleener.civ@mail.mil**

**Marco Mayor**
**U.S. Army PEO STRI**
**Orlando, FL**
**marco.mayor.civ@mail.mil**

**Andrew Maxon**
**Cybernet Systems Corporation**
**Orlando, FL**
**amaxon@cybernet.com**

## ABSTRACT

There are a number of upcoming paradigm shifts within Information Assurance (IA), to include policy and technical mandates, affecting IA in today's training and simulation systems. Maintaining situational awareness of a system's IA posture has been a challenge DoD wide. Specifically, in the training and simulation community it has been especially difficult given the closed, restricted networks the systems create or may intermittently traverse. A number of DoD wide policies and technical solutions have been developed and procured to ensure a system owner has continuous oversight of their system's IA posture. Over the years the Defense Information System Agency (DISA) has provided tools and solutions to Project Managers (PMs) to easily assess a given systems IA posture at a given time. The most popular example of these tools was the Gold Disk. However, the Gold Disk program was discontinued in 2012. Next came a suite of products much more scalable and robust in capabilities, but also with significant complexity. Assured Compliance Assessment Solution (ACAS), Host Based Security System (HBSS), and Continuous Monitoring and Risk Scoring (CMRS) are a few of the latest DISA licensed Commercial Off The Shelf (COTS) and Government Off The Shelf (GOTS) solutions available to PMs for integration into their systems at no cost. These solutions were designed for an enterprise Information Technology (IT) environment, but must be scaled to integrate with training and simulation systems. This paper will discuss the continuous monitoring requirements, benefits, emerging security practices, implementation concepts, and a training system example. This paper will document how the U.S. Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI) is addressing the growing cybersecurity threats through continuous monitoring and improved situational awareness by leveraging DISA licensed COTS and GOTS solutions to secure training and simulation systems. All DISA licensed COTS and GOTS described in this paper are available at no cost to the Government to implement.

## ABOUT THE AUTHOR

**Mr. Graham Fleener** is the IA Manager (IAM) for Project Manager Training Devices (PM TRADE) in the U.S. Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI). Mr. Fleener served in the U.S. Marine Corps and then worked as a contractor for the Army before joining the Army Acquisition Corps as a Government employee. Mr. Fleener obtained both his Project Management Professional (PMP®) and Certified Information Systems Security Professional (CISSP®) certifications. Mr. Fleener holds a Bachelor of Science in Information Systems Technology from the University of Central Florida and a Master of Science in Modeling and Simulation from the University of Central Florida.

**Mr. Marco Mayor** works as an Information Security Analyst for the Chief Information Office (CIO) in the U.S. Army Program Executive Office for Simulation, Training, and Instrumentation (PEO STRI). Mr. Mayor worked four years as an Information Assurance Analyst and then transitioned to Government civil service as a certifier. Mr. Mayor holds multiple industry certifications including the CompTIA Security+, Certified Ethical Hacker (CEH), and Certified Information Systems Security Professional (CISSP®). He holds a Bachelor of Science in Information Technology (IT) from the University of Central Florida and is currently pursuing a Master of Science in Modeling and Simulation from the University of Central Florida.

**Mr. Andrew Maxon** is the Cyber Security Division Manager for Cybernet Systems. He holds a Bachelor of Science in Information Systems Technology from the University of Central Florida with a focus in Network Security and has multiple industry certifications including the CompTIA Security +. He has certified and accredited numerous training and simulation systems for the U.S. Army, U.S. Navy, U.S. Marine Corp, and currently manages all Information Assurance Certification and Accreditation activities for Cybernet's government contracts.

# Continuous Monitoring of Cybersecurity in a Training System Environment

**Graham Fleener**
**U.S. Army PEO STRI**
**Orlando, FL**
**graham.g.fleener@mail.mil**

**Marco Mayor**
**U.S. Army PEO STRI**
**Orlando, FL**
**marco.mayor.civ@mail.mil**

**Andrew Maxon**
**Cybernet Systems Corporation**
**Orlando, FL**
**amaxon@cybernet.com**

## INTRODUCTION

The Department of Defense's (DoD) approach to Information Assurance (IA) has previously been a static and sequential process that culminated in an accreditation decision. Figure 1, Current Defense Information Assurance Certification and Accreditation Process (DIACAP) vs. Future Risk Management Framework (RMF), depicts how the affirmation of the accreditation decision, referred to as an Authorization To Operate (ATO), was maintained by time driven milestones such as IA Vulnerability Alert (IAVA) updates, annual security reviews, and triennial reaccreditations. This process succeeded in bringing many previously unsecure systems into compliance. However, this process has a number of areas for refinement in today's highly dynamic cybersecurity landscape.

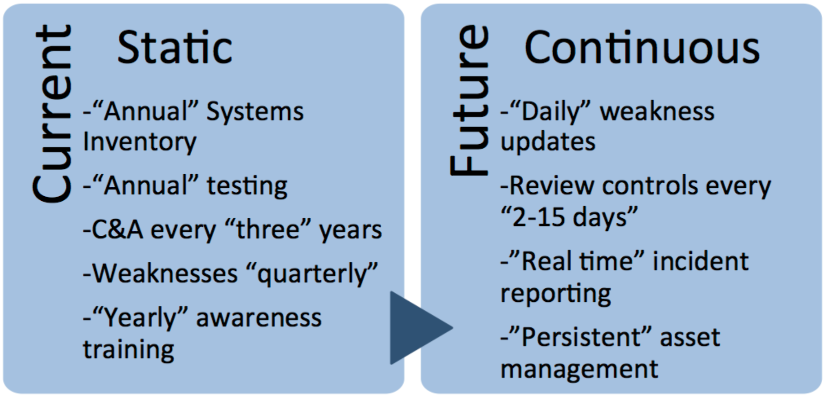

Current
Static
-"Annual" Systems Inventory
-"Annual" testing
-C&A every "three" years
-Weaknesses "quarterly"
-"Yearly" awareness training
Future
Continuous
-"Daily" weakness updates
-Review controls every "2-15 days"
-"Real time" incident reporting
-"Persistent" asset management

**Figure 1. Current Defense Information Assurance Certification and Accreditation Process (DIACAP) vs. Future Risk Management Framework RMF**

The most recent initiatives by the DoD have been to mitigate the risk of Project Managers (PM) preparing their systems to be inspection ready just prior to a milestone event. In addition, it has been a challenge for a PM to assess the compliance and risk level of a system at a given time. This is especially prevalent on a training system that may have limited or no connectivity to the outside world, yet still has significant data to protect. PEO STRI has fielded a number of training systems with no Global Information Grid (GIG) connectivity or that only communicate on closed, restricted training networks. Given the closed infrastructure of many training systems, continuous situational awareness of the cybersecurity compliance is a significant technical and manpower challenge.

To accomplish the continuous monitoring and improved situational awareness initiative, the DoD has produced a number of guidance documents and procured enterprise license agreements for Commercial Off The Shelf (COTS) software to enable continuous monitoring of cybersecurity risks and threats within a system. The predecessor to this Software was the DoD Government Off The Shelf (GOTS) tool Gold Disk. The Gold Disk program was ended in 2012. The new line of COTS tools for cybersecurity are much more complex and powerful, yet labor intensive in both implementation and sustainment.

This paper will discuss the requirement for continuous monitoring within the DoD, and more specifically training systems. In addition, this paper will review the benefits to both the end user and the system owner for enabling overall situational awareness of cybersecurity. Conversely, this paper will highlight many of the challenges, costs, and limitations associated with the DISA licensed GOTS and COTS tools. There will be an example discussed from an implementation within a classified training system. From the authors' experience on both instances, the paper will discuss best practices and lessons learned associated with implementation and sustainment. Finally, the paper will review some of the future work necessary within training systems to achieve the end goal of situational awareness for cybersecurity.

## CONTINUOUS MONITORING REQUIREMENT

In testimony to the House Committee on Oversight in 2010, the United States Chief Information Officer (CIO) Vivek Kundra, first outlined the need for continuous monitoring of "security-related information from across the enterprise in a manageable and actionable way" (Kundra, 2010). Figure 2, Continuous Monitoring Requirements Evolution, depicts the timeline for the continuous monitoring requirement. Kundra discussed the need for continuous monitoring as a means to "effectively transform an otherwise static security control assessment and risk determination process into a dynamic process" (Kundra, 2010). As a concept, continuous monitoring was deployed to not only provide security related feedback to the system owner, but also to enable a means to take action against a threat or vulnerability. Additionally, it would allow system owners to dynamically assess risk in a more fluid manner than the previous process.

The requirement was then put into legislation through the National Defense Authorization Act for Fiscal Year (FY) 2011. In that legislation continuous monitoring required the DoD "to achieve, to the extent practicable, the automation of continuous monitoring of the effectiveness of the information security policies, procedures, and practices within the information infrastructure of the Department of Defense, and the compliance of that infrastructure with such policies, procedures, and practices" (United States Code, 2011).

Continuous monitoring requirements have now been written into DoD Instructions. The latest requirements for cybersecurity and risk management include planning for continuous monitoring as stated in DoD Instruction (DoDI) 8510.01, "Continuous monitoring capabilities will be implemented to the greatest extent possible" (Department of Defense, 2014). Additionally, DoDI 8510.01 discusses "developing and documenting a system-level strategy for continuous monitoring of the effectiveness of security controls" (Department of Defense, 2014). The system-level continuous monitoring strategy will also be required to "align and conform with DoD enterprise-level and DoD component level continuous monitoring strategies" (Department of Defense, 2014).

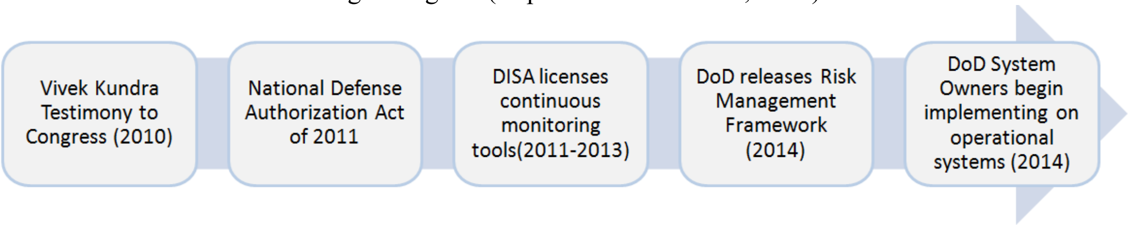

Vivek Kundra Testimony to Congress (2010)
National Defense Authorization Act of 2011
DISA licenses continuous monitoring tools(2011-2013)
DoD releases Risk Management Framework (2014)
DoD System Owners begin implementing on operational systems (2014)

**Figure 2. Continuous Monitoring Requirements Evolution**

## BENEFITS OUTSIDE OF INFORMATION SECURITY

The primary reason for implementing a continuous monitoring strategy is to reduce the overall technical risk to a system. However, there are a number of second and third order effects implementation could have on a system. First, the ability to track and inventory software, hardware, and licenses will be simplified. The continuous monitoring software has asset tracking capabilities that simplify a system owner's inventory and logistics processes. Second, greater automation of tasks such as network scans and vulnerability data collection reduces the potential for human error that was present in previously manual, time consuming tasks. Third, configuration management of standalone systems can be challenging when administered remotely. For example, PEO STRI has a number of isolated and standalone systems that need to ensure configuration management is tightly controlled. With continuous monitoring sensors deployed, compliance of approved configuration baselines becomes achievable. Fourth, from a long-term perspective there is the opportunity to reduce the sustainment IA labor hours required to maintain a system. For example, the number of tasks required for an IA analyst on a system will be reduced through automation as stated in

National Institute of Standards and Technology (NIST) Special Publication 800-137, “through the use of automation, it is possible to monitor a greater number of security metrics with fewer resources, higher frequencies, larger sample sizes, and with greater consistency and reliability than is feasible using manual processes” (NIST, 2011).

The final and potentially most significant reason for a continuous monitoring implementation is to reduce the number of time driven IA milestones that only provide a snapshot in time and not a true assessment of the risk of a system. RMF is set to replace the (DIACAP) in late 2014. In the upcoming RMF, there is a concept called ongoing authorization. Currently, PEO STRI systems are typically accredited under a type accreditation that must be reaccredited every three years. An ongoing accreditation would allow a system owner to maintain the system without a formal reaccreditation as long as a number of conditions are met. NIST describes ongoing accreditation as when “the authorizing official maintains sufficient knowledge of the current security state of the information system (including the effectiveness of the security controls employed within and inherited by the system) to determine whether continued operation is acceptable based on ongoing risk determinations, and if not, which step or steps in the RMF needs to be re-executed in order to adequately mitigate the additional risk” (NIST, 2010). To achieve an ongoing accreditation, a “robust and comprehensive continuous monitoring strategy integrated into the organization’s system development life cycle process” (NIST, 2010) is required. Figure 3, PEO STRI IA Milestone Schedule, illustrates the events and milestones an ongoing authorization could potentially eliminate. In the initial acquisition the milestones as documented below will still be performed to ensure compliance during the procurement. However, SP 800-37 describes an ongoing authorization as one in which the Authorizing Official (AO) would have the ability to make a decision on what “steps would need to be re-executed” (NIST, 2010).

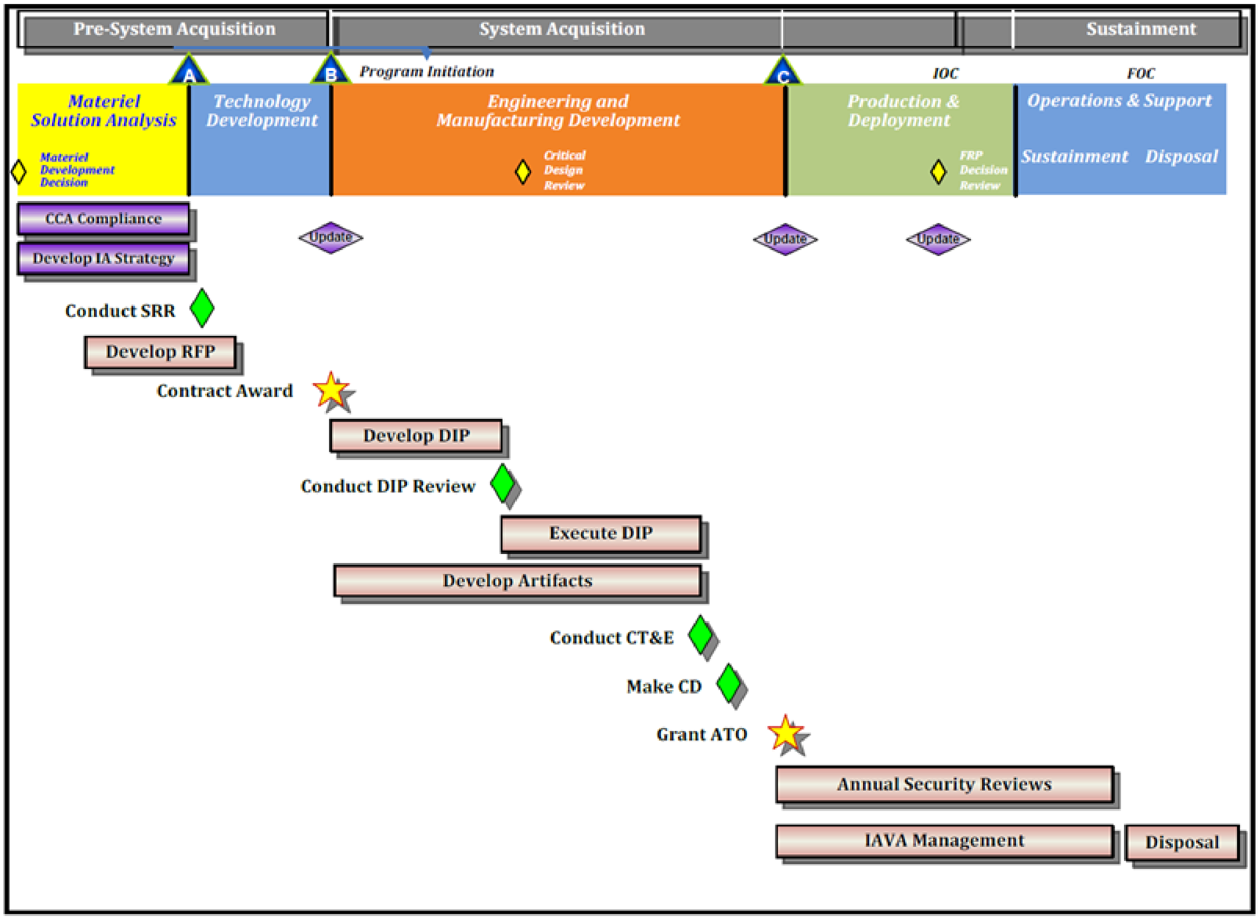


**Figure 3. PEO STRI IA Milestone Schedule**

## EMERGING SECURITY PRACTICES

In order to implement the continuous monitoring requirement, DoD has combined three emerging security practices tasked with the sole purpose to provide training systems with near-real time IA situational awareness. These applications are the Assured Compliance Assessment Solution (ACAS), Host Based Security System (HBSS), and the Continuous Monitoring Risk Scoring (CMRS) system. The next sections, will explain what they are, what components they are made of and how they all work together.

### ACAS

The Defense Information System Agency (DISA) provides the ACAS suite at no cost to DoD agencies. It is a scalable suite of COTS applications, which has the ability to provide automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, Security Technical Implementation Guides (STIG) compliance, and network discovery (ACAS, 2014). Table 1, ACAS Components, explains the ACAS components, including its main application SecurityCenter, which is a free of cost COTS application, available to government civilians, and contractors supporting government programs.

**Table 1. ACAS Components**

| | |
|---|---|
| **SecurityCenter** | It works as the central console for the ACAS architecture. It manages Nessus Policies, scanning assets, alerts, reports, and plugin updates across the enterprise. |
| **Nessus** | A multi-platform vulnerability scanner, which will be replacing its predecessor Retina. Nessus supports the Security Content Automation Protocol (SCAP) which allows the STIG verification. It also verifies the Information Assurance Vulnerability Management (IAVM) compliance. |
| **Passive Vulnerability Scanner (PVS)** | The PVS monitors network traffic in real-time. It is constantly looking for new hosts, new applications and new vulnerabilities. It determines server and client side vulnerabilities and sends these to SecurityCenter in real-time. |
| **3D Tool** | This tool is a topology viewer which provides graphical analysis information such as network and protocol maps, communication paths, and vulnerability maps. It imports asset data from the Nessus scanners or the SecurityCenter console. |
| **XTool** | In earlier versions of SecurityCenter, The XTool was used to convert distributed eXtensible Checklist Configurations Description Format (XCCDF) files, or STIG benchmarks into Extensible Markup Language (XML) schema, allowing the files to be imported into SecurityCenter. Today, you can import these XCCDF files directly into SecurityCenter and the XTool is no longer required (ACAS-Components, 2014). |

The ACAS suite can be implemented by running a kickstart installation (SecurityCenter) or by executing individual installation packages (all other components). ACAS can be installed in a laptop, desktop, or server. After a fresh installation, the SecurityCenter implementation complies with most of the DoD security requirements. Once installed, a manual security review is still required. The ACAS license must be renewed yearly, and government contractors shall make the license request directly through their government point of contact. Figure 4, ACAS Architecture, displays the relationship of each ACAS software components (Nessus, PVS, xTool, and 3D Tool) and its central console SecurityCenter.

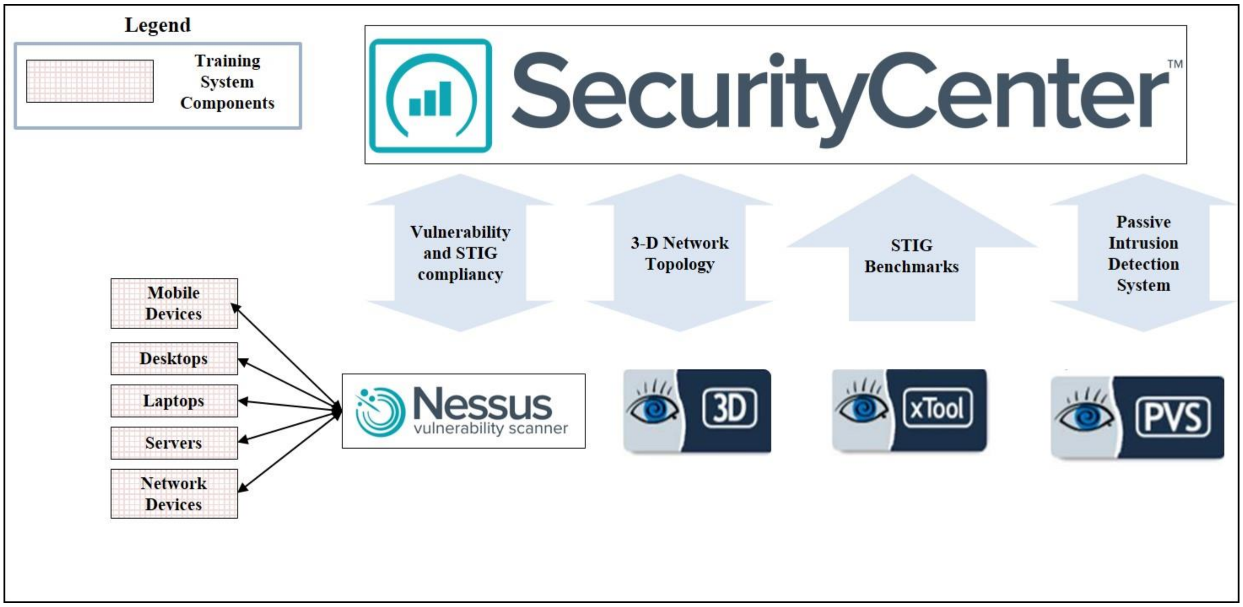

Legend
Training System Components
SecurityCenter™
Vulnerability and STIG compliancy
3-D Network Topology
STIG Benchmarks
Passive Intrusion Detection System
Mobile Devices
Desktops
Laptops
Servers
Network Devices
Nessus vulnerability scanner
3D
xTool
PVS

**Figure 4. ACAS Architecture**

## HBSS

The HBSS suite is provided at no cost to DoD agencies by DISA, and it comes in the form of a pre-configured image (ePO server) and individual installation packages (all other point components). HBSS is a COTS suite of software applications that monitor, detect, and counter against acknowledged cyber-threats to DoD systems and networks. Unlike ACAS, the HBSS solution is installed on each host (server, desktop, and laptop) in DoD. The HBSS solution is normally managed by local administrators and configured to address known exploit traffic using an Intrusion Prevention System (IPS) and a host firewall. After a fresh installation, the HBSS implementation complies with most of the DoD security requirements. Once installed, a manual security review is still required. (HBSS, 2014).

HBSS is composed of management, endpoint, and reporting components. Table 2, HBSS Management Components, explains the three management components, which handle the suite management and deployment.

**Table 2 - HBSS Management Components**

| | |
|---|---|
| **ePolicy Orchestrator (ePO) Management Suite** | The Central management application. It's in charge of the installation, management and configuration of the HBSS components. It also provides system administrators the capability of viewing reports to help monitor deployments, vulnerabilities and protection levels. |
| **McAfee Agent (MA)** | The agent provides secure communication for policy enforcement locally on endpoints. It communicates to ePO for the latest policy updates, and sends events from HBSS endpoint products to ePO. |
| **SIM Connector** | Enables real-time attack detection and diagnosis, providing situational awareness. |

Table 3, HBSS Endpoint Protection Components, explains the five endpoint protection components, which are installed directly on the hosts. These components report current baselines, virus attacks, rogue network components, rogue devices, and system snapshots up to the ePO Server.

**Table 3 - HBSS Endpoint Protection Components**

| | |
|---|---|
| **Antivirus (AV)** | This component comes in two flavors; McAfee VirusScan Enterprise (VSE) and Symantec Endpoint Protection (SEP). Both applications provide protection against viruses, Trojan horses, worms, bots, and rootkits. |
| **Host Intrusion Prevention System (HIPS)** | This capability provides a host intrusion detection/prevention system (IDS/IPS) along with a firewall. |
| **Rogue System Detection (RDS)** | Detects unknown systems such as workstations, servers, and printers. |
| **Data Loss Prevention (DLP)/Device Control Module (DCM)** | This is primarily used to prevent USB storage drives to be mounted on hosts. |
| **Asset Baseline Monitor (ABM)** | This module scans systems to provide system snapshots of critical files, configuration and registry settings in order to detect tampering and alteration. |

Table 4, HBSS Reporting Components, explains the three reporting components, which may reside in the ePO server itself, or in the hosts. These components report asset specific information, asset compliance data, and keep track of asset inventory.

**Table 4 - HBSS Reporting Components**

| | |
|---|---|
| **Asset Publishing Service (APS)** | Publishes HBSS asset, software, and compliance data to CMRS with supporting operational information (owning organization, location, system, etc.) |
| **Operational Attribute Module (OAM)** | Allows assets managed by an ePO to be associated with the functional owner attributes such as combatant commands, Services, agencies and field activities. |
| **Asset Configuration Compliance Module (ACCM)** | Gathers detailed asset inventory on all hosts and provides near-real time situational awareness of asset inventory. |

Figure 5, HBSS Architecture, displays the hosts with all the HBSS components installed, as well as the data provided to the HBSS ePO Server.

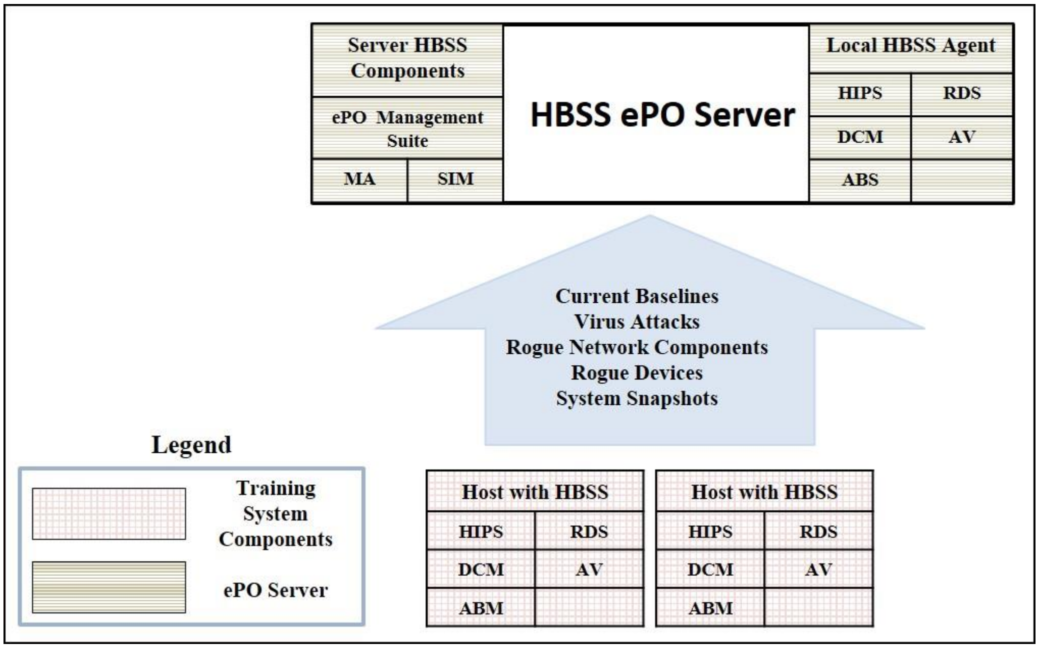


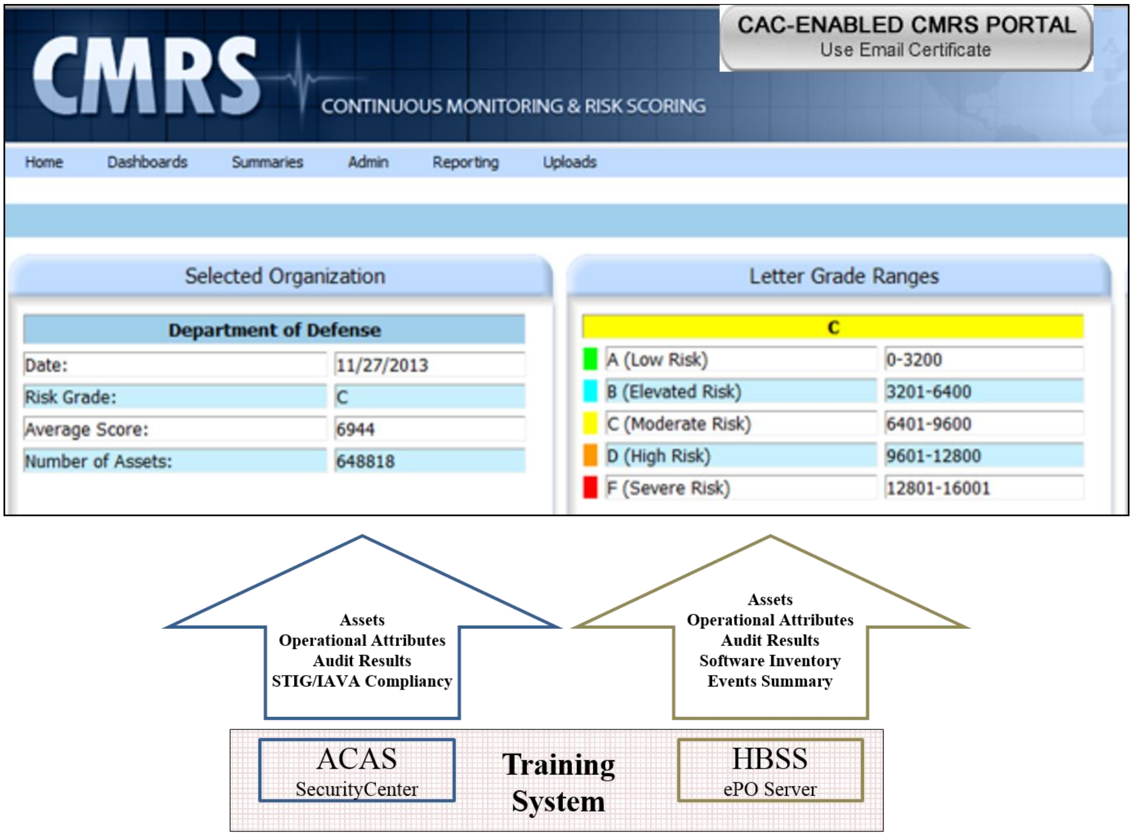
**Figure 5. HBSS Architecture**

**CMRS**

CMRS suite is provided at no cost to DoD agencies by DISA. It is web-based system that visualizes and quantifies the cybersecurity risk of the DoD based on published asset inventory (provided by HBSS) and the compliance data (provided by ACAS), via usage of a dashboard. CMRS allows users to gather decision-making information, implement prioritized mitigation decisions, and ensure effectiveness of security controls in order to support their cybersecurity risk management duties (CMRS, 2014). By using CMRS, network defenders will be able to determine if their assets are configured securely. If their configuration has changed, it will provide them with situational awareness on how to effectively apply cyber defense resources.

The Enterprise User Management (EUM) is the main component to the CMRS. It is a web-based module that provides the capability to create new accounts, manage account permissions and profile information for CMRS. The main concern with CMRS is data confidentiality. DISA addresses this issue by implementing role-based permissions to enforce need-to-know access to CMRS data. Users must complete a CMRS Access Request Form 2875. Each organization is assigned a trusted agent. This trusted agent reviews the CMRS Access Request Form, and grants or denies access. If access is granted, users authenticate the site via Common Access Card (CAC) and a Personal Identification Number (PIN).

In order for CMRS to work, HBSS and ACAS data must be imported into CMRS. This data is evaluated and computed by CMRS, where an average risk score of zero means no calculated risk and the maximum average risk score for an organization is 16000 for HBSS data and 8000 for ACAS data. Figure 6, CMRS Implementation with ACAS and HBSS, highlights the relationship between ACAS, HBSS, and CMRS. It shows the different types of data provided by ACAS and HBSS up to CMRS.



Department of Defense

| | |
|---|---|
| Date: | 11/27/2013 |
| Risk Grade: | C |
| Average Score: | 6944 |
| Number of Assets: | 648818 |

C

| | |
|---|---|
| 🟩 A (Low Risk) | 0-3200 |
| 🟦 B (Elevated Risk) | 3201-6400 |
| 🟨 C (Moderate Risk) | 6401-9600 |
| 🟧 D (High Risk) | 9601-12800 |
| 🟥 F (Severe Risk) | 12801-16001 |

**Figure 6. CMRS Implementation with ACAS and HBSS**

## SECURITY RELATED BENEFITS AND THREAT MITIGATIONS

If configured correctly, the three emerging solutions (CMRS, ACAS and HBSS) can help training systems reduce the insider threat, provide the capability to detect vulnerabilities near real-time, and help maintain a robust IA posture. This section will document an overview of how each of the threat mitigations provides a security benefit.

### Reduce Insider Threat

Since 2010, insider threats climbed to the top in the list of cybersecurity issues the Pentagon has had to deal with. As in the case of PFC Bradley Manning who downloaded classified files from military networks, burned the files to a CD, and leaked them to WikiLeaks. Another infamous insider threat activity was the one by the former National Security Agency (NSA) contractor Edward Snowden. He transferred classified information to a thumb drive about how the agency tracks domestic call data and foreigners' Internet activities. According to an article published by Nextgov.com, an NSA information technology official, who left the organization in 2012, said that at the time HBSS was not installed. This application would have mitigated the risk of using removable storage devices such as CDs, thumb drives, etc. (Sternstein, 2013).

If HBSS is installed in training systems, it can disable all write privileges (including downloads) to all forms of removable media devices and block privileged users from accessing sensitive data. Although HBSS is known to be a powerful countermeasure tool against known threats, it is important to remember that HBSS can only protect networks to the extent of their configuration. These technical controls coupled with administrative controls, such as signed User Access Privilege (UAP) and Privileged Access Agreement (PAA) forms, can help reduce the insider threat.

### Passive and Active Vulnerability Monitoring Provides Early Detection Capabilities

The Passive Vulnerability Scanner (PVS) application, mentioned in table 1, can monitor network traffic in training systems in real-time and in a non-intrusive manner. HBSS can address unusual traffic on network hosts via the different endpoint protection components mentioned in table 3. These HBSS modules can be configured to simply monitor and detect vulnerabilities (passive), or to block attacks from rogue hosts immediately (active). Neither the PVS nor the endpoint protection modules, affect the training system performance.

### IA Posture Continuous Awareness

Both ACAS and HBSS feed data or reports up to CMRS in an XML format. The CMRS reports can be scheduled for automatic publishing and/or manual uploading. The purpose is to increase situational awareness and hence maintain a more continuous compliant state. Continuous monitoring ensures ongoing effectiveness of cybersecurity and risk management governance, mission/business processes, enterprise and security architectures, and security controls deployed within the enterprise.

## CONTINUOUS MONITORING FOR STANDALONE AND SYSTEMS WITH LIMITED CONNECTIVITY

Currently, these continuous monitoring practices are implemented in connected DoD networks. The challenge DoD faces, is ensuring standalone training system and systems with limited connectivity comply with the continuous monitoring requirement. Figure 7, Manual CMRS Update Process, explains the process proposed by DISA for standalone systems. It involves sneaker netting XML ACAS and HBSS feeds manually through the CMRS portal. Even though, this process involves exporting data, burning it on portable media, and then uploading it to CMRS, it is the only way to keep these systems isolated, while meeting the continuous monitoring requirement.

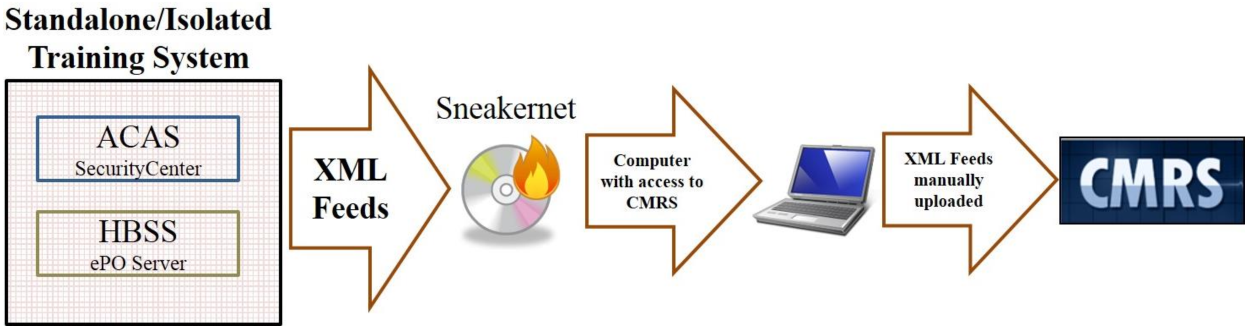

Standalone/Isolated Training System
ACAS
SecurityCenter
HBSS
ePO Server
XML Feeds
Sneakernet
Computer with access to CMRS
XML Feeds manually uploaded
CMRS

**Figure 7. Manual CMRS Update Process**

## TRAINING SYSTEM EXAMPLE

We analyzed a high fidelity ship bridge simulator that integrates multiple training sub-systems into one homogenous virtual training environment, providing training for all bridge crew roles. The specific trainers are one of a kind trainers and are the only platforms available on which bridge crews can train. The actual ships do not support on-ship training. Crews must fully certify for duty via virtual training only. The reliance on virtual training enforces the need to continuously monitor the IA posture of the network and computers for malicious activity that could cause disruptions to training schedules and readiness. To combat these threats and reduce risk, continuous monitoring capabilities were integrated into all systems within the IA accreditation boundary.

These bridge trainers use a typical simulator design running a mix of Windows and Linux operating systems, with roughly 30-50 computers within their IA accreditation boundaries. HBSS was one of several tools used within the training system in order to improve situational awareness, reduce insider threats, and gain control over the IA posture. An HBSS ePO Server was integrated into the trainer networks and HBSS agents were deployed to all IA-enabled Windows and Linux computers within the accreditation boundary. Modules and components were installed and configured for AV, HIPS, DLP/DCM, ABM, and Policy Auditor. The process from design to software request and implementation of the HBSS suite provided valuable insight into the realm of Enterprise level Continuous Monitoring and Control within a training environment. Many challenges were experienced with licensing, performance, hardware requirements, application complexity, and costs (acquisition and ongoing lifecycle maintenance).

### Licensing

The first immediate challenge confronted was licensing of the software. HBSS components such as McAfee ePO and its underlying modules are free to government Project Managers (PM) via government Enterprise Licensing Agreements (ELAs). Although HBSS is available at no cost on government contracts, there are components that require additional licensing to be purchased, these include but are not limited to, Red Hat Enterprise Linux (RHEL), Microsoft Server, Microsoft SQL server, and/or Client Access Licenses (CALs). Once the appropriate licenses are provided to the government and requests for software are approved, a self-installation DVD is created and returned to the contractor for implementation. This DVD is used to install a pre-configured image of the HBSS ePO server into the Environment (Microsoft Hyper-V, VMWare ESXi, or physical installation). Both Virtual and Physical server installations are available, but the environment must be decided before making the request. Once delivered to the government, it is the government’s responsibility to purchase updates to licensing. Early design planning can help to keep licensing costs to manageable levels.

### Performance

Continuous monitoring can greatly affect performance in several areas. Careful consideration must be given to the continuous monitoring server’s performance needs, taking into account dual roles it might be serving for other IA tasks such as backups and updates. A major performance factor to take into account when deploying HBSS agents are identifying which HBSS modules could negatively affect system performance. HBSS agents can take up significant resources when executing different policies, such as scanning for system vulnerabilities, applying updates, or analyzing network traffic. Careful attention should be given to the scheduling of these policies. The performance hit is negligible on standard enterprise based workloads involving email, Internet, and Microsoft Office. However, high fidelity simulations can substantially drain available system resources. HBSS agents running in the background have the potential to utilize a vast amount of system resources causing further degradation to the simulation and a possible loss of trainer functionality. When taking into account these agents might be executing policies while running high fidelity simulations, more thought needs to be given to the proper configuration of each agent, module, and policy.

### Hardware Requirements

The additional performance overhead of continuous monitoring can force the need to upgrade hardware. Many times this is an afterthought and hardware is upgraded shortly after deploying continuous monitoring capabilities in order to combat performance issues that arise. Understanding how to size up your system and hardware requirements can be difficult. HBSS ePO Server is normally provided as a Virtual Machine, but in most scenarios will require an additional full time server. Hardware requirements can differ greatly depending on the number of computers within the accreditation boundary and the services provided. Additionally, other IA roles such as backups and updates can have impacts on hardware requirements. If implementing the full suite of ACAS, HBSS, and CMRS into a large network, multiple servers may be needed. Once all the continuous monitoring applications have been installed, they need to be configured properly and tuned to get the best performance out of the system.

### Application Complexity

Continuous Monitoring offers the system administrator greater oversight of a network, but it does so at the cost of increased application complexity. The large suite of overly complex applications and processes require a higher skill level to maintain than a standard network administrator. HBSS alone has nearly a dozen different modules with complex menus and various options. There is so much granularity when creating reports and modifying plugins that administrators can get caught up in information overload. It can be extremely difficult to discern what information is important when flipping between multiple application consoles and interfaces. Additionally, when validating the vulnerability status of systems, detailed settings need to be communicated between the validating parties. Using incorrect parameters can greatly reduce your risk posture and score. The trio of continuous monitoring applications comes with a large learning curve and multiple weeks of training are needed to help master each suite of applications. However, these classes can be costly and time consuming, often driving up acquisition and maintenance costs. IA training for continuous monitoring applications targeting onsite maintainers and ISEOs has recently started to appear in government requirements but training times can be too short and lacking detail, barely scratching the surface for most applications. As continuous monitoring capabilities expand within training systems, additional funding will be needed to support IA training for onsite maintainers.

### Cost

Increased costs can be tied too all of the above challenges. The DOD maintains a large amount of standalone and closed network environments. This is done for various reasons including budget, classification level, and location. Many times it can be impractical to integrate a Continuous Monitoring server into a standalone trainer that consists of only one computer or a small network of computers. Maintaining connections to the GIG and the cost of IA in those situations can bump up against budget constraints in an era when most government programs are trying to do more with less. Standalone and closed environments can further increase costs through manual labor needed to move data between networks. Classification levels can make it extremely difficult to export regular reporting data, requiring administrators to sneaker-net classified data between networks. These issues compound themselves when the training systems are deployed to remote locations, far away from landline connections for data and power. There are implementation costs for software licensing and hardware needed to run the multiple suites of applications, which increase as the number of clients increase. Application complexity drives the need for additional application specific IA maintenance training. This need for longer and more detailed IA training requirements will continue to drive up acquisition costs. Continuous monitoring will help increase situational awareness and reduce insider threats, but it will do so at a cost. Careful consideration of these design challenges, along with a cost benefit analysis will help keep continuous monitoring projects within scope and budget.

## FUTURE CHALLENGES AND WORK

There is a vast amount of future work that will need to take place before the DoD receives the full benefit from continuous monitoring tools, processes, and policies. At the PEO STRI level, we will be moving beyond pilot programs and into a more broad deployment of the software suites described in this paper. Additionally, PEO STRI will be implementing the Risk Management Framework (RMF) with Army CIO/G-6 guidance in the next Fiscal Year (FY). The software suites will be refined to provide metrics to not just the DoD level, but also the local PEO STRI level to ensure we can react efficiently with threats, vulnerabilities, and compliance. As contractors and Government agencies become more experienced, the software configurations and capabilities will equally become more refined, efficient, and cost effective.

## REFERENCES

Defense Information Systems Agency. (2014). *ACAS*. Retrieved on February 25, 2014, from http://www.disa.mil/Services/Information-Assurance/ACAS

Defense Information Systems Agency. (2014). *ACAS Components*. Retrieved on February 26, 2014, from https://east1.deps.mil/disa/cop/mae/netops/acas/SitePages/Components.aspx

Defense Information Systems Agency. (2014). *CMRS*. Retrieved on March 15, 2014, from https://east1.deps.mil/disa/cop/mae/netops/CMRS/SitePages/Home.aspx

Defense Information Systems Agency. (2014). *HBSS*. Retrieved on February 28, 2014, from http://www.disa.mil/Services/Information-Assurance/HBSS

Defense Information Systems Agency. (2014). *HBSS Components*. Retrieved on March 16, 2014, from https://east1.deps.mil/disa/cop/mae/CyberDefense/HBSS/SitePages/Components.aspx

Department of Defense. (2014). *Risk Management Framework (RMF) for DoD Information Technology (IT) Instruction 8510.01.* Retrieved April 17, 2014 from http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

Kundra, Vivek. (2010). *Testimony Federal Information Security*. Retrieved April 11, 2014 from https://cio.gov/vivek-kundra-testimony-federal-information-security/

National Institute of Standards and Technology. (2011). *Information Security Continuous Monitoring Special Publication 800-137*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf

National Institute of Standards and Technology. (2010). *Guide for Applying the Risk Management Framework to Federal Information Systems Publication 800-37*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

Sternstein, A. (2013). *Pentagon spent millions to counter insider threats after WikiLeaks fiasco*. Retrieved on March 16, 2014 from http://www.nextgov.com/cybersecurity/2013/07/defense-spent-millions-counter-insider-threats-after-wikileaks-fiasco/65843/

United States Code. (2011) *Title 10*. Retrieved on April 11, 2014 from http://www.gpo.gov/fdsys/pkg/USCODE-2011-title10/pdf/USCODE-2011-title10-subtitleA-partIV-chap131-sec2223a.pdf