



**HIT Standards Committee Security Hearing**  
**Talking Points**  
*Systems Stability and Reliability Panel*



**(1) Briefly describe your organization and your information security approach to system stability and reliability.**

The Department of Veterans Affairs (VA) is responsible for administering benefits programs for veterans, their families, and survivors. The organization consists of medical centers, community-based outpatient clinics, veteran centers, regional offices, and national cemeteries. There are currently 7.84 million enrollees in the VA Healthcare System and the Agency holds tremendous amounts of financial, health, and personal information for our nation's veterans and their families.

The VA is the only federal agency with a centralized Office of Information and Technology (OI&T) that not only manages all the IT employees but budget as well. This is significant because centralization enables the Agency to more effectively manage its information security program by allowing for increased accountability and standardization of security processes. Within OI&T, the Office of Information Protection and Risk Management (IPRM) is responsible for driving the information security program, through our 450 information security officers located at VA facilities across the country. IPRM's mission is to serve our veterans, their beneficiaries, employees, and all VA stakeholders by ensuring the confidentiality, integrity, and availability of VA sensitive information and information systems.

Our security approach is to balance information protection with information access. VA must safeguard veteran, beneficiary, and employee sensitive information while continuing to provide high quality services to veterans and their beneficiaries. IPRM maintains veteran needs while protecting VA's sensitive data by enacting strong information protection and risk management processes and procedures.

**(2) Provide one or two examples of information security issues you have faced recently related to system stability and reliability, and describe how you addressed these issues.**

In 2005, Hurricane Katrina separated thousands of New Orleans evacuees from their healthcare providers and medical charts. VA efforts to maintain appropriate and uninterrupted care to evacuated veterans were supported by nationwide access to comprehensive electronic health record (HER) systems. Enrolled veterans' electronic clinical records were available from the rehosted Veterans Health Information Systems and Technology Architecture (VistA) system to authorized users with access to VA's secure network. The Agency was able to successfully meet immediate patient care data needs and provide continuity of operations using its EHR system and derivative data. Additional methods used by VA to assist in continuing patient care include use of a regional data warehouse, as well as a master patient index and locator via VistAWeb.

After the Katrina experience, VA staff implemented new methods to ensure uninterrupted availability to VistA data. These new techniques, which combine routine backups and continuous data feeds to remote rehost sites, were used within weeks in preparation for hurricanes Rita and Wilma.

**(3) What kinds of trade-off's have you had to make between security and usability, and other operational considerations?**

The implementation of security tools affects network performance. As security levels are increased and protection becomes salient through inspection of larger amounts of network traffic, the network performance is affected. To mitigate this issue, network resilience and redundancy must be increased and the costs for construction and maintenance follow.

Security systems also affect usability and work patterns of VA customers and employees, and these factors must be considered when implementing security standards. Homeland Security Presidential Directive (HSPD)-12 Personal Identity Verification (PIV) implementation is an example of a security standard and its associated technical systems that must be implemented in a balance of security layers and user practicality. A doctor or nurse at a medical center uses his or her PIV card for authentication into IT and medical systems. The time needed to log into systems and insert cards into readers can have a negative impact on patient care or become a barrier in an emergency situation. Cards may also be left unattended in computers, unintentionally granting full access to VA resources. Also, if an employee forgets their card, they will be prevented from gaining access to necessary systems.

Veterans accessing VA resources are another example of a tradeoff between usability and security. Accessing sensitive information through Web portals such as My HealthVet require security configurations and standards that adequately protect the health and identity information of the user, along with the integrity of VA systems. The information must be provided across the Internet through secure communications methods that require no applications or major configuration changes to the public computer. Currently, veterans are required to visit a VA benefit or medical center so that their identity can be confirmed and username/password combinations can be given for access. The resources and time dedicated by both employees and veterans for authentication ensure security but are not always convenient.

**(4) What information security standards are you currently using to meet your business needs for system stability and reliability?**

VA follows National Institute for Standards and Technology (NIST) guidance, Office of Management and Budget (OMB) memorandum, HSPDs, Executive Orders, Government Accountability Office (GAO) reports and other federal and industry guidance. Examples include the Federal Information Security Management Act of 2002 (FISMA); Veterans Benefits, Healthcare, and Information Technology Act of 2006 (PL 109-461); HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*; NIST 800 Series Special Publications; and Consensus Audit Guidelines (CAG)-20, *Critical Security Controls for Windows*, developed by the SANS Institute.

**(5) What challenges have you had to address in implementing these standards (e.g., training)?**

VA has faced challenges implementing multiple security tools which often have conflicts on the network. Due to the nature of VA's mission, we are specifically affected by the security standards associated with medical devices. The issue stems from the inability to enforce enterprise security policies on medical products whose design and operation are regulated by the Food and Drug Administration (FDA) and cannot be modified by the end user. For example, medical devices can restrict the application of operating system patches and malware protection updates. VA is currently implementing a Medical Device Isolation Architecture (MDIA) that uses firewalls to allow medical devices to communicate while maintaining best security and networking practices.

The VA Health Information Security Division (HISD) and VHA Biomedical Engineering segregate medical equipment on virtual local area networks (VLANs) so that our active scanning of computers does not interfere with medical procedures. However, VA faces challenges when facilities do not keep this separation of duties. For instance, the Agency recently discovered an infection of medical requirement at a VA facility and as a result, needed to clean the infection and certify or re-certify the equipment. As a result, we just published the VA Medical Device Isolation Architecture Guideline 2009 to provide a standard process for isolating and securing networked medical devices using a protected Virtual Local Area Network (VLAN) structure. This document presents a six step process for identifying, grouping, and migrating networked medical devices to an isolated VLAN infrastructure. This process includes the following:

1. Device Identification
2. Grouping and Segmentation
3. Identify Communication Requirements
4. Migration Planning and Coordination
5. System Migration
6. Implementing Protection

Furthermore, VA's mission is geared towards healthcare, and exchanging data such as EHRs over our network is a daily activity. The Agency has faced challenges in building data centers using VistA because it was not designed for the capacity for which we currently use it. For example, VistA was never designed to provide seamless support for large-scale disasters such as Hurricane Katrina. VA staff constantly needs to modify back-up systems and applications, as well as send data feeds to remote rehost sites, to ensure uninterrupted data availability.

**(6) What is the role/value of interoperable information security standards in helping assure system stability and reliability?**

An increase in interoperable information security standards would lead to a higher level of system stability and reliability. For example, multiple security vendors provide tools that have their own language. Interoperable standards would allow different systems from different vendors to operate together in a security suite. Increased interoperability among industry and security reporting standards would make it easier for federal agencies to integrate tools into their system and therefore improve system stability and reliability.

**(7) What are the current limitations or gaps in interoperable information security standards with respect to system stability and reliability?**

As we look to develop enterprise-wide public and private health networks for exchanging EHRs, there is not a standard in existence that requires uniform reporting for organizations to report a security incident. Some organizations are required to report an incident within an hour, while others may have 24 hours to do so. There is a critical need for standardization in this area because without it, there are tremendous implications if a network goes down or there is a large data breach and no one reports it for 24 hours.

**(8) What new and emerging issues around system stability and reliability do you foresee over the next 2-3 years?**

Bandwidth demands will increase as virtualization and cloud computing grow in application and use. The amount of bandwidth needed by security products and tools to communicate with management consoles and SEMs across the network is also a concern. Log retention, network scanning, and real-time monitoring systems all need increasing amounts of bandwidth which could ultimately affect network performance and safety of live IT resources. A balance must be found between the amount of security information collected from network elements and the performance of the network. There is a need for seamless integration of security systems and tools, business practices, and usability. Security needs to be transparent to the user and minimally impact network performance and reliability.

Additionally, protection of critical network infrastructure will be a challenge in the coming years. Power supply and cooling system improvement in VA data centers and improvement of physical and environmental systems that protect critical network infrastructure at medical centers will be needed. As virtualization and server consolidation become standards, the reduction in the amount of systems and rack space utilized should help to improve power consumption and cooling system demand.