

# Enterprise Cybersecurity Strategy

## *Protecting Veteran Information and VA Data*

VA's Office of Information and Technology (OI&T) is evolving into a world-class organization that enables delivery of healthcare and benefits to Veterans through state-of-the-art technology. VA OI&T's actionable, far-reaching Enterprise Cybersecurity Strategy demonstrates the organization's commitment to protecting Veteran information and VA data, while meeting the MyVA goal to provide Veterans with access to their information when and where they need it most. The strategy, which was delivered to Congress on Sept. 28, 2015, establishes an ambitious and carefully crafted approach to cybersecurity and privacy protections.

### **Significance and Five Strategic Goals**

Safeguarding Veteran information and VA data is essential to providing quality health care, benefits, and services to our Nation's Veterans. The Enterprise Cybersecurity Strategy will guide VA's plan for implementing the actions, processes, and organization that will achieve these five strategic goals:

- Protecting Veteran information and VA data
- Defending VA's cyberspace ecosystem
- Protecting VA infrastructure and assets
- Enabling effective operations
- Recruiting and retaining a talented cybersecurity workforce

### **How is this strategy different from VA's previous approach to cybersecurity?**

*"MyVA represents an opportunity to affect fundamental changes in VA's systems and structures to align with our mission and values. The MyVA vision is to provide a seamless, unified Veteran Experience across the entire organization and throughout the country. "*

— Secretary Bob McDonald

This Enterprise Cybersecurity Strategy strengthens VA's defensive and offensive cybersecurity posture. It is focused on building a comprehensive cybersecurity capability that supports VA's overall MyVA transformation effort. Our approach will initiate policy changes and accelerate existing work to tighten current security gaps and strengthen VA's cybersecurity posture.

### **The VA enterprise is a complex organization. How does this approach ensure maximum security of Veteran information and VA data?**

Information technology (IT) is an enabler of each of VA's lines of business, and our plan considers this complexity. The Enterprise Cybersecurity Strategy is comprehensive in scope, taking into account current and future external IT factors, such as the consumerism of IT and the Internet of Things, and their potential impact on VA's continued growth. Our approach stresses defense in depth — a layering of people, processes, technologies training, and operations — to achieve more secure VA information systems, from mobile devices to desktops to data centers. To ensure that our intent becomes reality, OI&T is working as a cross-functional team with our VA, public sector, and industry partners to translate goals and objectives into discrete actions, initiatives, and innovations for which the organization will be held accountable.

## **How is the Enterprise Cybersecurity Strategy protecting Veteran information and VA data from future cyberthreats?**

Priority has been given to near-term actions that strengthen our current cybersecurity environment — but we recognize that as we continue to evolve, cyberthreats do also. That is why we have created an Enterprise Cybersecurity Strategy Team focusing on eight domains — governance, program management, and risk management; operations, telecommunications, and network security; security architecture; application and software design; privacy; access control, identification and authentication; cybersecurity training and human capital; and medical cyber — and will continuously work to monitor threats and identify the newest technologies and best ways to secure VA’s IT infrastructure.

### **Does the VA’s plan align with federal government cybersecurity guidelines?**

Yes, the Enterprise Cybersecurity Strategy encompasses enhancements needed in each of the fundamental domains of cybersecurity and effectively implements security controls specified for federal government systems by the Office of Management and Budget and the National Institute of Standards and Technology. It includes key objectives specified by the Federal CIO in addition to those specific to VA. The plan also includes

steps and actions necessary to achieve the Cross-Agency Priority (CAP) Goal for cybersecurity. Established by the Government Performance and Results Modernization Act of 2010, CAP goals are tools used by leadership to accelerate progress on a limited number of Presidential priority areas – such as cybersecurity – where implementation requires active collaboration between multiple agencies.

### **What is the time frame for the implementation plan?**

Implementation of the Enterprise Cybersecurity Strategy is underway for 16 objectives aligned with the five strategic cybersecurity goals. The strategy is to be realized in the now (July 2015 through January 2016), near (January through July 2016), and future (August 2016 and beyond) timeframes.

Objectives completed by the end of January 2016 include the establishment of a full Enterprise Security Architecture team, completion of a security program dedicated to telemedicine, and implementation of a Security Operations Center that provides a focused incident response capability for timely detection and remediation of threats to VA’s network.

Medical cyber includes medical devices that can be networked or accessed electronically. Just like servers that collect and transmit personally identifiable information and protected health information, these IT-enabled and networked medical devices must be protected from exploitation and from becoming operable vectors for cyberattacks. Medical cyber will expand over time to encompass protections for all “cyber physical” systems with similar electronic characteristics, such as industrial control and elevator systems.