

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 health care and benefits to Veterans through state-of-the-art technology. OI&T's actionable, far-reaching Enterprise Cybersecurity Strategy and implementation plan demonstrate the organization's commitment to protecting Veteran information and VA data and limiting access to only those with the proper security credentials. 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?

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 close current security gaps and strengthen VA's future cybersecurity posture.

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

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 such external factors as the consumerism of IT and the "Internet of Things." Our approach stresses defense in depth — a layering of people, processes, technologies and operations — to achieve more secure VA information systems, from mobile devices and desktops to data centers, with an emphasis on employee training and continuous education. 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 develop a detailed implementation plan that will translate goals and objectives into discrete actions, initiatives, and innovations for which the department 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's why we've created Enterprise Cybersecurity Strategy teams. These teams each focus on one of eight domains — including privacy, security architecture, 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 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. The plan also includes steps and actions necessary to achieve the Cross-Agency Priority Goal for cybersecurity.

What is the time frame for the implementation plan?

Implementation of the Enterprise Cybersecurity Strategy has already begun. VA’s OI&T already has 21 projects in action, as outlined in the strategy, as of September 2015.