

INTRODUCTION TO CYBERSECURITY

VOLUME 5, ISSUE 2

OFFICE OF INFORMATION AND TECHNOLOGY (OIT)

INTRODUCTION

In ancient times, defenders built stone walls; today, they build [firewalls](#) to protect from an extensive repertoire of methods attackers use to breach both. Some techniques never change: ancient attackers sometimes had infiltrators within the fortress, or they'd trick defenders into letting them in. Present day, insider threats and [Trojan Horse](#) programs remain two of the most serious information technology (IT) security risks amidst a sea of cyber threats. Cybersecurity, also referred to as IT security, focuses on protecting computers, networks, programs, and data from unintended or unauthorized access, change, or destruction. In this Tech Insight, we present an overview of cybersecurity and security controls, as well the Department of Veterans Affairs' (VA) strategy to combat cybersecurity risks, including VA's Enterprise Architecture (EA) and Cybersecurity Strategy.

OVERVIEW OF CYBERSECURITY

Cybersecurity protects the data and integrity of computing assets belonging to or connecting to an organization's network. Its purpose is to defend those assets against all threat actors throughout the entire life cycle of a cyber attack. Cybersecurity is very important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. Organizations transmit sensitive data across networks in the course of doing business, which require protection as the volume and sophistication of cyber attacks grows. Elements of cybersecurity include network security, application security, cloud security, identity management, mobile security, etc.

According to the [Department of Homeland Security \(DHS\)](#), "Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks." Globally, technology is more interconnected than ever before, and to complicate matters further, cybersecurity threats change from year to year.

According to the Chief Security Officer (CSO) from [International Data Group \(IDG\)](#), which “serves enterprise security decision-makers and users with the critical information they need to stay ahead of evolving threats and defend against criminal cyberattacks,” [predictions for 2018](#) include the following threats:

- Artificial intelligence (AI) powered attacks via spam/fraud/phishing messaging, AI-powered password guessing, etc.
- Reduced sandboxing technologies effectiveness as attackers find more ways to defeat sandboxing, thereby requiring an additional layer of technology
- Cyber-hijacking
- More compliance regulations after high profile breaches in 2017
- Cyberwar as we see a further escalation of international conflict in cyberspace
- Attacks against cyber currencies and blockchain systems

OVERVIEW OF SECURITY CONTROLS

In combatting cybersecurity and any other IT/security risk, VA must comply with a plethora of different policies including the [National Institute of Standards and Technology \(NIST\)](#), Health Insurance Portability and Accountability Act of 1996 (HIPAA), [Federal Information Security Modernization Act of 2014 \(FISMA\)](#), and others. In addition, configuration baselines, which are documented, up-to-date specification to which the information system is built, must be considered. They adhere to standards set by Federal Desktop Core Configurations (FDCC), United States Government Configuration Baseline (USGCB), and Defense Information Systems Agencies (DISA) Security Technical Implementation Guides (STIGs) per [VA Handbook 6500](#). Configuration baselines provide information about the components of an information system, network topology, and the logical placement of the component within the system architecture. VA Handbook 6500 is the primary source for information security policy and is built on [NIST 800-53](#), *Recommended Security Controls for Federal Information Systems*.

Compliance alone is not enough, and solutions must align to VA’s risk management strategy in both design and operation. Furthermore, with so many different compliance requirements and technologies to be secured, secure solution design can be overwhelming and challenging at times. You may be wondering, can EA provide a solution?

VA’S ENTERPRISE ARCHITECTURE

The VA EA comprises the strategic, business, data and information, systems and applications, network and infrastructure, and security information used by decision-makers within VA. VA EA can help align solutions to VA’s enterprise strategy as well as meet compliance objectives and

best practices such as the National Security Agency (NSA) [Community Gold Standards](#). VA EA's security domain works to protect VA's infrastructure, assets, networks, systems, and data. VA is working to protect all Veteran information and VA data and limiting access to only those with the proper authority.

VA EA can provide assistance at three levels – strategy with goals and objectives; design with [Enterprise Technical Architecture \(ETA\)](#); and technology with approved standards, technology, and [One VA Technical Reference Model \(TRM\)](#). VA's [Enterprise Shared Services \(ESS\)](#) provides further assistance by providing resources that have already been designed to be secure and compliant with a VA authority to operate (ATO) allowing solutions to inherit security controls.

Continuous monitoring is required by the [Federal Risk and Authorization Management Program \(FedRAMP\)](#) for each IT service in order to maintain an ATO. A reference architecture for cloud security guidelines is located in the [Cloud Security Enterprise Design Pattern \(EDP\)](#). Also, the security classification of each IT service is based on a review of the business requirements and impacts to mission and business processes in the event of a security breach or disaster. Each mission system that is registered in the VA Systems Inventory (VASI) is required to complete a business impact analysis (BIA) to determine the appropriate security controls.

VA'S CYBERSECURITY STRATEGY

VA's Enterprise Cybersecurity Strategy (ECSS) directs VA leadership to act as cybersecurity resource stewards to identify and articulate requirements, standards, and opportunities for transformative cybersecurity improvements. ECSS is focused on building a comprehensive cybersecurity capability predicated on protecting and countering the spectrum of threat profiles through a multi-layered defense. The ECSS includes the following five strategic goals: 1. Protecting Veteran information and VA data; 2. Defending VA's cyberspace ecosystem; 3. Protecting VA infrastructure and assets; 4. Enabling effective operations; and 5. Recruiting and retaining a talented cybersecurity workforce.

Mr. Scott Blackburn, Executive in Charge for Information and Technology and Chief Information Officer for the Office of Information and Technology (OIT), provided [testimony on Dec. 7, 2017](#) where he discussed VA's commitment to "our continuing effort to improve Enterprise Cybersecurity. VA's Enterprise Cybersecurity Strategy will ensure that Veteran data is secure, available, and safe from cyber threats. Safeguarding Veteran information and VA data is essential to providing quality health care, benefits, and services to our Nation's Veterans.....Our strategy establishes an ambitious yet carefully-crafted approach to cybersecurity and privacy protections that helps VA to execute its mission of providing quality health care, benefits, and

services to Veterans, while delivering on our promise to keep Veteran information and VA data safe and secure.”

Building upon current VA initiatives, VA’s implementation plan entitled the [VA Enterprise Cybersecurity Strategy Plan \(ECSP\)](#), leverages best practices from private sector, other Federal agencies, and recognized standards organizations, such as [Comprehensive National Cybersecurity Initiative](#) (CNCI), which consists of a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace, and [Federal Information Security Modernization Act of 2014 \(FISMA 2014\)](#). The plan will make use of innovative commercial security strategies widely adopted as security best practices across the commercial and government sectors. Furthermore, the implementation plan incorporates lessons learned from actual response and recovery efforts to Federal cyber incidents and input from Federal agencies.

The ECSP will help VA to “make prioritized, defensible decisions related to the implementation of cybersecurity projects (that may be technical or procedure-based), align programmatic activities with the NIST Cybersecurity Framework (CSF), and create an integrated and transparent program across each level of the program, which includes Government-wide statutory requirements, VA policy and implementation guidance, organizational cybersecurity capabilities, mission/business processes, and the information system level,” according to Mr. Blackburn.

CONCLUSION

Cybersecurity threats are increasing at an alarming rate in our digital world. To further complicate the issue, the types of threats and approaches to maintain our security are also constantly evolving. NIST recently issued guidelines in its [Framework for Improving Critical Infrastructure Cybersecurity](#) that recommends a shift toward continuous monitoring and real-time assessments, a data-focused approach to security. The question for you to consider is how VA’s cybersecurity strategy will amidst the numerous security controls and whether it can be the solution that will protect Veterans and their data.

TECH INSIGHT SERIES

The monthly Tech Insight series aims to help readers make better decisions and be more informed customers (of Office of Information and Technology’s, or OIT, products and services) by providing them with high-level overviews of technology issues that impact or will impact VA’s Information Technology (IT) environment. Tech Insights introduce topics in an easily digestible fashion by presenting background information on the topic, clearly explaining its importance within VA, and providing recommendations for success from OIT. View all Tech Insights [here](#).

DISCLAIMER: This document includes links to websites outside VA control and jurisdiction. VA is not responsible for the privacy practices or the content of non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected and how it is used.