

DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INFORMATION AND TECHNOLOGY



ENTERPRISE CYBERSECURITY STRATEGY

SEPTEMBER 2015

PAGE INTENTIONALLY LEFT BLANK

Department of Veterans Affairs Enterprise Cybersecurity Strategy

CHIEF INFORMATION OFFICER'S MESSAGE

Veterans depend on the Department of Veterans Affairs (VA) to protect the information they have entrusted to our organization. Safeguarding Veteran information and VA data is intrinsic to providing quality healthcare, benefits, and services to Veterans. With this commitment in mind, I am pleased to present VA's Enterprise Cybersecurity Strategy.

I am focused on leading VA's Office of Information & Technology (OI&T) through a transformation where we will become an organization that is transparent, accountable, innovative, and teamwork oriented. Throughout this transformation, our number one priority is the Veteran – ensuring a safe and secure environment for their information, and approaching the security of Veteran data from the Veteran's point of view in concert with Secretary McDonald's MyVA strategy.



In today's internet-based information technology (IT) environment, cybersecurity for our critical infrastructure, assets, networks, systems, and data is one of the most significant challenges our country faces. Every day, our Nation experiences increasingly sophisticated cyber threats and malicious intrusions that are politically- or economically-motivated, causing individuals to experience identity theft at record levels. The emergence of cybersecurity challenges, as well as innovative technologies and new capabilities, presents unprecedented challenges and opportunities for VA. The Department must balance these challenges and opportunities as we constantly improve upon the delivery of services and benefits to Veterans and their families.

IT is an enabler of each of VA's disparate lines of business, including the largest integrated healthcare system in the United States; a benefits processing organization equivalent to a medium-size insurance company; the largest integrated memorial and cemetery organization in the country; a court system; and many other components. Recognizing this complexity, one of my first acts as Chief Information Officer was the formation of an Enterprise Cybersecurity Strategy Team (ECST) responsible for delivering an actionable, long-range, cybersecurity strategy and implementation plan for VA.

The strategy considers VA's complexity and multitude of functions while continuously adapting to the newest technologies and the best way to secure VA's IT infrastructure. The strategy takes a broad approach, involving state, local, Federal, and private sector partners, as well as the American public. The strategy also provides the Department an executable path to ensure we are delivering on our promise to keep sensitive data safe and secure.

The strategy identifies five distinct goals critical to success: **Protecting Veteran Information and VA Data, Defending VA's Cyberspace Ecosystem, Protecting VA Infrastructure and Assets, Enabling Effective Operations, and Recruiting and Retaining a Talented Cybersecurity Workforce.** The strategy also details a number of cross-cutting factors to enable VA's long-term success.

To ensure our intent becomes reality, OI&T is working as a cross-functional team with our VA, public, and industry partners to develop a detailed implementation plan that will translate our goals and objectives into discrete actions, initiatives, and innovations for which the organization will be held accountable. The implementation plan will also be an enabler to the MyVA vision of providing excellent customer service to Veterans in a safe and secure manner.

I wish to express my appreciation to the team who dedicated an incredible amount of time and energy into creating this strategy. Continuing our proud history of serving America’s Veterans and their families is at the forefront of what we do each day. Veterans are counting on us to deliver on the strategy and implementation plan so they can feel confident in the safety of VA data and systems.

Thank you,

LaVerne H. Council
Assistant Secretary for Information and Technology and Chief Information Officer



EXECUTIVE SUMMARY

VA is committed to protecting all Veteran information and VA data and limiting access to only those with the proper authority. Meeting this commitment requires a comprehensive strategic approach that spans VA and the cyberspace ecosystem in which Veterans, VA, and VA's partners operate. By its very nature, the Internet is an open system facilitating the free flow and exchange of information, ideas, and commerce, embodying some of the very principles upon which this Nation was founded. The very same qualities are accompanied by a growing number of vulnerabilities and risks threatening our Nation's security, stability, and prosperity.

“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

VA, its core constituents, and external partners are all subject to a wide variety of these threats. Given the high degree of connectivity, mutual interdependence, and reliance on integrated open platform technology, meeting cybersecurity challenges requires dedicated strategic attention. VA's Enterprise Cybersecurity Strategy is focused on building a comprehensive cybersecurity capability supportive of VA's overall transformation effort to secure the execution of the MyVA mission as it modernizes VA technical culture, processes and capabilities. The strategy is predicated on protecting and countering the spectrum of threat profiles through a multi-layered defense in depth model enabled through five strategic goals.

1. Protecting Veteran Information and VA Data: Ensuring secure technology and data systems to protect all VA data is insufficient in and of itself. Equally important is ensuring privacy concerns such as those enacted in law are addressed (e.g., Health Insurance Portability and Accountability Act (HIPAA)). Examining VA business processes and human interactions (Veterans, beneficiaries, employees, contractors, partners, etc.) is critical to building the greater defensive depth necessary to address both security and privacy.

- 2. Defending VA's Cyberspace Ecosystem:** Providing secure and resilient VA information systems technology, business applications, publically accessible platforms, and shared data networks is central to VA's ability to defend VA's cyberspace ecosystem. Addressing technology needs and operations that require protection, rapid response protocols, and efficient restoration techniques is core to effective defense.
- 3. Protecting VA Infrastructure and Assets:** Protecting VA infrastructure requires going beyond the technology and systems wholly owned and operated by VA within its facilities to include the boundary environments that provide potential access and entry into VA by cyber adversaries.
- 4. Enabling Effective Operations:** Operating effectively within the cybersphere requires improving governance and organizational alignment at enterprise, operational, and tactical levels (points of service interactions). This requires VA to integrate its cyberspace and security capabilities and outcomes within larger governance, business operation, and technology architecture frameworks.

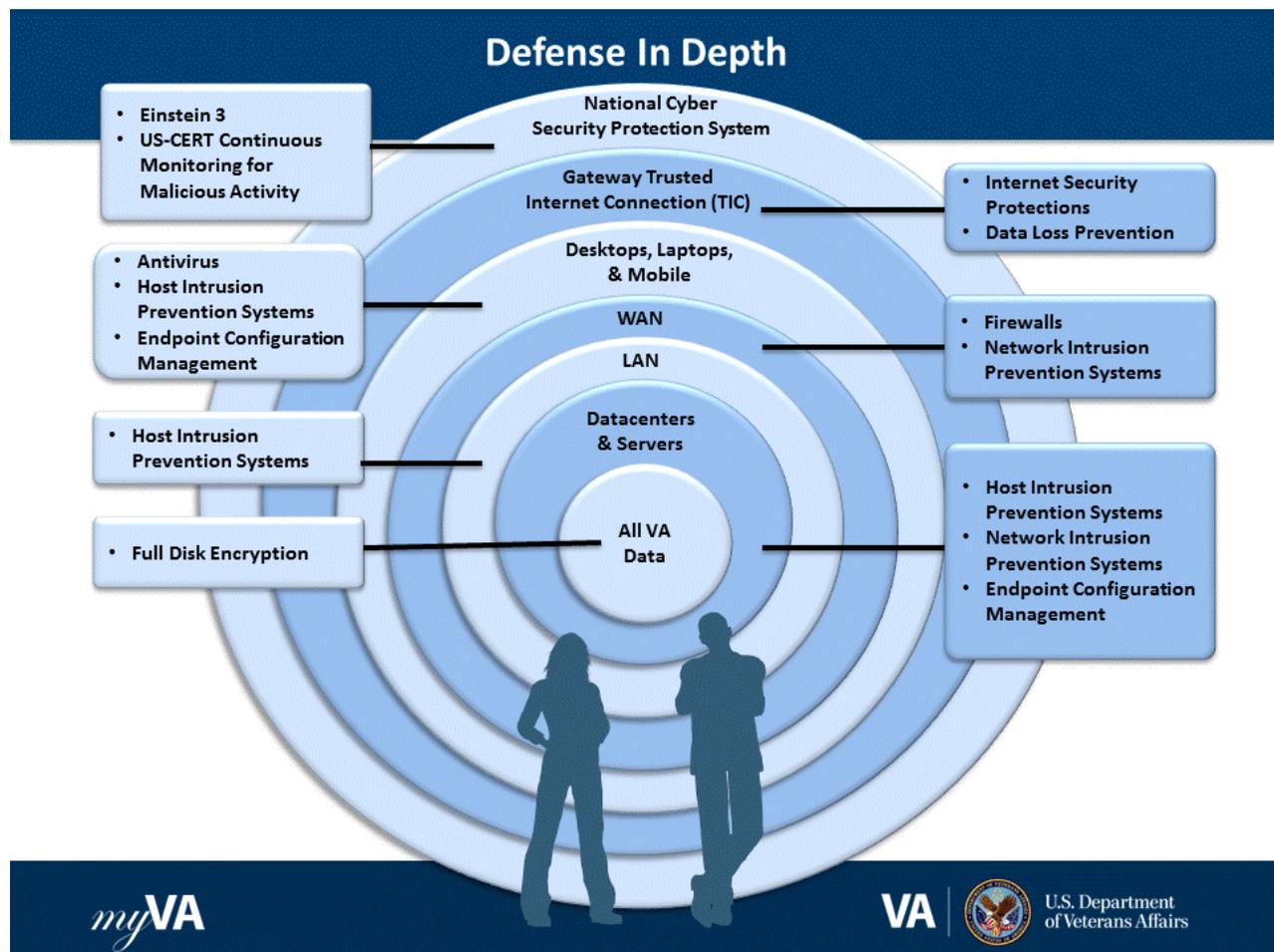
5. ***Recruiting and Retaining a Talented Cybersecurity Workforce:*** Strong cybersecurity requires building a workforce with talent in cybersecurity disciplines to implement and maintain the right processes, procedures, and tools. A well-functioning security organization requires a blend of technical, policy, and leadership resources covering multiple disciplines within cybersecurity and maintaining pace with the growing dependence on technology for mission essential activities.

BACKGROUND

The enterprise cybersecurity strategy will guide VA's plan to implement the actions, processes, and organization that will deliver the 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**
5. **Recruiting and Retaining a Talented Cybersecurity Workforce**

While the enterprise cybersecurity strategy and implementation plan cover a broad range of actions and expectations, the overall intent is to better defend all VA data and information assets, improve identification and detection of vulnerabilities and threats, and mature response and recovery capabilities for enhanced readiness and resilience when incidents inevitably arise by addressing VA's longstanding material weaknesses. The approach emphasizes defense in depth – a layering of people, processes, technologies, and operations – to achieve more secure VA information systems.



VA must also anticipate attacks and incorporate procedures for response and recovery to achieve strong security. Implementing the plan will not prevent every cyber incident. In fact, as improvements are made to VA defenses and detection tools are added to our IT systems, additional and previously unknown malicious activity will likely be discovered. However, the end result will be more secure VA assets allowing VA to balance cherished values around privacy and civil liberties with measures protecting the confidentiality, integrity and availability of Veteran’s information.



Understanding VA’s environment, identifying and addressing the strengths, weakness, resources, constraints, capabilities, and drivers are paramount. Coupling this with VA’s known and unknown threats informs a credible and achievable risk mitigation plan. This in-depth understanding of organizational risks and vulnerabilities, paired with known current threats and the most effective policies and technologies for addressing them, also provides an understanding of any resource constraints that may hinder our progress.

The rapid expansion of cyber technology in our modern world has created paradigm shifts in how individuals, commercial entities, academia, non-profits, and governments interact. Coupled with other emergent technologies, the pace of change is driving tectonic shifts in the global economy, resulting in unprecedented productivity gains and efficiencies.

Over the years, VA researchers nationwide have worked on thousands of studies at VA to advance medical science treatment and technology. The list of accomplishments includes: the implantable cardiac pacemaker; computerized axial tomography (CAT) scans; functional electrical stimulation systems that allow patients to move paralyzed limbs; the nicotine patch; and the first electronic ankle-foot prosthesis.

Forward progress, though, brings risks that are increasingly varied in nature, widespread in reach, and severe in impacts when not effectively countered. In the Federal government, agency IT systems, information/data, and infrastructure assets are continually attacked and exploited by hostile actors, both internal and external. Whether the intents are inadvertent, deliberate, or malicious; or the sources are individuals, criminal enterprises, or even foreign governments; our Federal government assets and infrastructure are under increasingly intense assault.

VA and its partners are responsible for protecting the integrity, confidentiality, and availability of Veteran information and VA data, with VA ensuring its systems, networks, and operational processes are protected from a broad and increasingly complex spectrum of threats. VA’s Enterprise Cybersecurity Strategy details the approach and initiatives to respond to these threats.

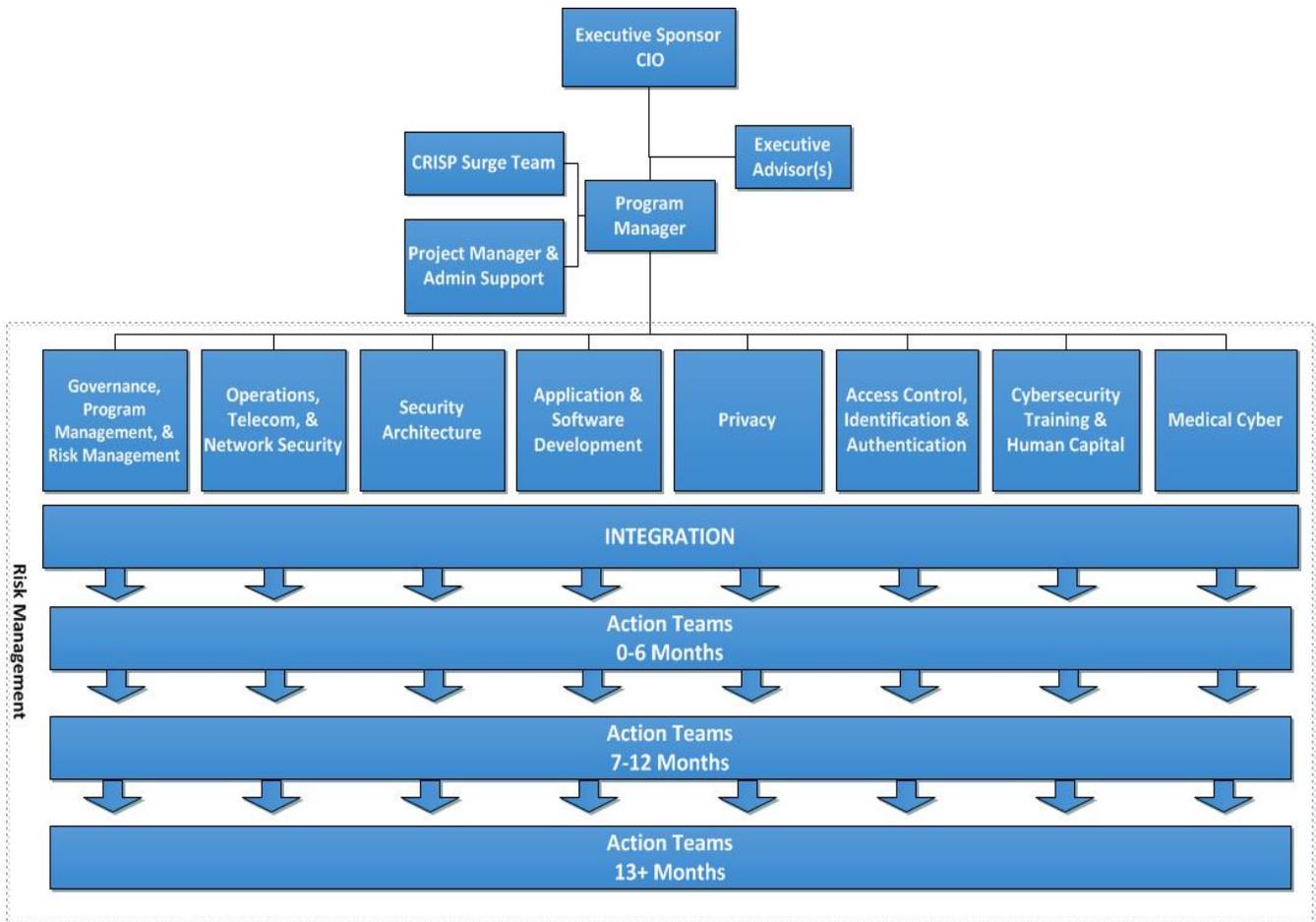
“In this interconnected, digital world, there are going to be opportunities for hackers to engage in cyber assaults both in the private sector and the public sector. Now, our first order of business is making sure that we do everything to harden sites and prevent those kinds of attacks from taking place.... But even as we get better, the hackers are going to get better, too. Some of them are going to be state actors; some of them are going to be non-state actors. All of them are going to be sophisticated and many of them can do some damage.”

– President Obama,

As VA progresses toward the desired future state, priority has been given to near-term actions to address material weakness conditions and implement continuous enhancements to VA systems as defense against cyber-attacks. The Enterprise Cybersecurity Strategy Team (ECST) will pursue practical and risk-based approaches on specific cyber defense strategies and actions needed to most effectively defend against the highest threats to VA’s mission and functions. This strategy will balance business needs with those of cybersecurity. Additionally, VA will focus on strategies for rapid recovery from any cybersecurity adverse incident. ECST consists of cross-functional IT teams working in the following eight domains and as illustrated in the subsequent diagram:

1. **Governance, Program Management, and Risk Management**
2. **Operations, Telecommunications (Telecom), and Network Security**
3. **Security Architecture**
4. **Application and Software Development**
5. **Privacy**
6. **Access Control, Identification (ID) and Authentication**
7. **Cybersecurity Training and Human Capital**
8. **Medical Cyber**

Enterprise Cybersecurity Strategy Team (ECST)



These eight domains will address findings from Office of Inspector General (OIG) Federal Information Security Modernization Act of 2014 (FISMA) audits and improve VA's future cybersecurity posture.

The success of a threat-based defensive approach hinges on cyber threat intelligence analysis, defensive engagement of the threat, and focused sharing and collaboration. Thus the scope of VA's Enterprise Cybersecurity Strategy includes all VA administrations.

VA's Enterprise Cybersecurity Strategy is designed to answer several critical questions:

- What are the right things to do to achieve our cybersecurity mission and vision?
- How do we know we are doing the right things?
- Are we making decisions and investments that deliver our cybersecurity strategy?
- Are we aligning our resources to deliver the strategy?
- Are we achieving intended outcomes?

VA's Enterprise Cybersecurity Strategy will guide VA's cybersecurity implementation plan. Building upon current VA initiatives, VA's implementation plan leverages best practices from private sector, other Federal agencies, and recognized standards organizations, such as the Comprehensive National Cybersecurity Initiative and FISMA. 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.

From a content perspective, VA's implementation plan will initiate policy changes, create new initiatives, and accelerate existing work with the overarching objective of closing current gaps and strengthening VA's cybersecurity environment. The plan specifies required capabilities, actions, milestones, and associated resource requirements. This encompasses enhancements needed in each of the fundamental domains of cybersecurity, while also effectively implementing security controls specified for Federal government systems by Office of Management and Budget and National Institute of Standards and Technology. The implementation plan also includes steps and actions necessary to:

- ✓ Achieve the President's Cross Agency Priority goals for cybersecurity
- ✓ Set clear direction through a structured framework (strategic roadmap)
- ✓ Clearly define success in terms of measurable outcomes mapped to specific initiatives that fulfill them
- ✓ Sequence key initiatives ready for action when funding, resources, and capacity are allocated

Collectively, all implementation plan elements will enable VA senior leadership to hold the organization accountable to achieving the Enterprise Cybersecurity Strategy's targeted outcomes.

STRATEGY

VA's Enterprise Cybersecurity Strategy is focused on building a comprehensive cybersecurity capability supportive of VA's overall transformation effort. VA's cybersecurity goals were shaped by several key influences:

- **Government-wide policy, standards and direction**
- **VA transformation and overall Strategic Plan goals and objectives**
- **General cybersecurity trends facing the enterprise**
- **Emerging technology disruptors on the horizon**

VA's infrastructure is vulnerable to a wide range of threats, both physical and cyber. This strategy is predicated on protecting and countering the spectrum of threat profiles through a multi-layered defense in depth model. This model will drive attainment of three critical strategic outcomes:

- **All Veteran information and VA data is protected and secure**
- **Federal government information and assets are protected and secure**
- **Veterans, users, and VA partners interact with VA and VA systems safely and securely**

VA's strategic outcomes are aligned with the five goals set forth by the Federal Chief Information Officer (CIO). A high-level overview outline of VA's cybersecurity goals and objectives is found below. Included are key objectives specified by the Federal CIO in addition to those specific to VA. Following the overview outline are detailed descriptions of each goal and objective. These are accompanied by specific strategies VA will undertake to attain each objective.

Overview Outline

- **Goal 1: Protecting Veteran Information and VA Data**
 - **Objective A:** Provide secure access and assure privacy protections
 - **Objective B:** Educate Veterans, external parties, and external users on safe information practices
 - **Objective C:** Strengthen business processes and supporting technology, including partner and third-party process interactions
- **Goal 2: Defending VA's Cyberspace Ecosystem**
 - **Objective A:** Enhance timely detection of cyber threats and intrusions and situational awareness
 - **Objective B:** Respond rapidly to cyber threats and intrusions through timely network monitoring and detection (includes wide-area network (WAN), Network Security Operations Center (NSOC), trusted internet connection (TIC), network mapping, etc.), intelligence sharing, and advanced threat analysis techniques
 - **Objective C:** Recover rapidly from cyber incidents through effective response, resilience, and restoration plans
 - **Objective D:** Manage risk by continuous monitoring, detection, and diagnostics; and accelerated adoption of lessons learned and mitigations

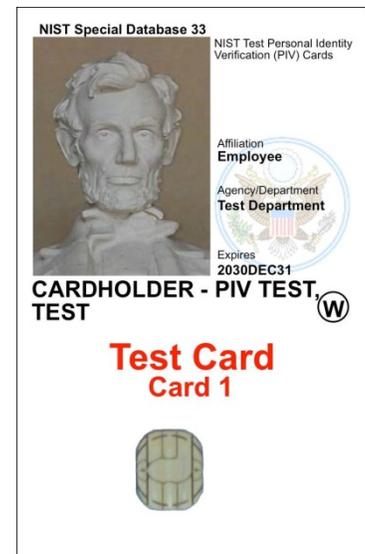


- **Goal 3: Protecting VA Infrastructure and Assets**
 - **Objective A:** Prioritize identification and protection of high value assets and sensitive information (local-area networks (LANs), data centers, servers, data, etc.)
 - **Objective B:** Incorporate security and privacy protections in VA’s environment
 - **Objective C:** Integrate security, application, and IT systems architectures
- **Goal 4: Enabling Effective Operations**
 - **Objective A:** Operate efficient and effective acquisition and deployment of emerging technology
 - **Objective B:** Conduct transparent and accountable operations
 - **Objective C:** Execute integrated governance
- **Goal 5: Recruiting, Developing, and Retaining a Talented Cybersecurity Workforce**
 - **Objective A:** Recruit, develop, and retain a world-class cybersecurity workforce
 - **Objective B:** Educate and train the VA workforce to engender a culture of cybersecurity
 - **Objective C:** Foster partner and supplier collaboration of our boundary environments on shared security and privacy goals and training options

Goals, Objectives, and Strategies – Descriptions and Definitions

Goal 1: *Protecting Veteran Information and VA Data*: Ensuring secure technology and data systems to protect all Veteran information and VA data is insufficient in and of itself. Equally important is ensuring privacy concerns such as those enacted in law are addressed (e.g., Health Insurance Portability and Accountability Act (HIPAA)). Examining VA business processes and human interactions (Veterans, beneficiaries, employees, contractors, partners, internal and external users), is critical to building the greater defensive depth necessary to address both security and privacy. This goal involves improving internal controls, business operations, and training of users, employees, and partners around securing Veteran information, improving general cyber “hygiene,” and appropriately addressing the privacy considerations of Veteran information and VA data. Additionally, it includes educating Veterans on actions they can take to secure their information in their interactions with VA and VA partners. This goal addresses the business intelligence required to actively monitor and understand attacker behaviors. By improving incident response processes, analyzing attack patterns, and sharing cyber intelligence, VA will gain actionable intelligence leading to a comprehensive understanding of threats and methods for defense.

- **Objective A: *Secure access and assure privacy protections*** – VA will improve the safeguards and privacy controls used by Veterans, external parties, and internal users to access, update, and use information to assure persons accessing VA systems are properly identified and have a right to access requested information, and support auditing. To meet this objective, VA will implement the following:
 - Evaluation and assessment of VA privacy posture and ensure messaging of VA privacy expectations
 - Enhanced personally identifiable information (PII) protections
 - Reduction of sensitive data holdings to improve VA’s risk posture by maintaining fewer instances of shared and duplicated data



- Identity access management of both users external and internal to VA (authentication, authorization, and access controls)
- Personal identification verification (PIV) badging for two-factor authentication (2FA) for all information domains across VA
- Role-based access controls
- **Objective B:** *Educate Veterans, external parties, and external users on safe information practices* – This objective is to improve the “hygiene” of how Veterans and users handle information to reduce risks and vulnerabilities their actions could introduce. To meet this objective, VA will implement the following:
 - Enhancement of access protocols for Veterans, external parties, internal and external users
 - Publishing of proper procedures and techniques for information handling
 - Expansion of outreach and education
- **Objective C:** *Strengthen business processes and supporting technology, including partner and third party process interactions* – Ensure interactions between Veterans, third parties, and VA business processes and systems employ safe information practices. To meet this objective, VA will implement the following:
 - Determination of single authoritative VA sources of identity information, contact information, demographic socio-economic data, and military service history (customer data integration)
 - Safe and secure business system designs for VA and partners
 - Secure interactions between VA and external parties
 - A culture of security across all business partners and third-party stakeholders
- **Goal 1 Targets:**
 - Veteran information and VA data is only accessed and released with proper authorization
 - Veteran information and VA data is 100 percent accessible to Veterans and authorized users in a secure manner
 - Privacy protections of Veteran information and VA data are fully in place
 - All actions to access resources or data can either be traced to an authenticated identity or flagged as anomalous and investigated
 - All actions that access resources or data take place in accordance with approved policy

“Nothing in IT is more important than protecting VA data and the information entrusted to us by Veterans.”

– LaVerne Council,
Assistant Secretary for
Information and
Technology and Chief
Information Officer

Goal 2: *Defending VA’s Cyberspace Ecosystem:* Providing secure and resilient VA information systems technology, business applications, publically accessible platforms and shared data networks is central to VA’s ability to defend VA’s cyberspace. This goal will address technology needs and operations that

require protection, rapid response protocols, and effective restoration techniques. This goal also focuses on incorporating a strong defense in VA's architecture to thwart attackers in their attempts to compromise Veteran information, VA data, and VA systems. This also includes building security into IT systems and services at the earliest stages of project initiation and developing defense in depth by an integrated architecture incorporating multiple layers of security. Defending VA's cyberspace requires attention to the ecosystem within which VA's cyber footprint operates. This goal will also address the vigilance and collaboration needed across VA's private and public partnerships to establish proactive defensive postures to prevent threats from materializing.

- **Objective A:** *Enhance timely detection of cyber threats and intrusions and situational awareness*— This objective will maintain a threat-focused orientation, improving VA's understanding of the external threat environment and providing actionable intelligence across VA's defensive cyber operations. To meet this objective, VA will implement the following:
 - Advanced network perimeter protection beyond the current signature-based approach performed for VA by Internet Service Providers
 - Passage of all traffic, including mobile and cloud, through TIC or managed trusted Internet protocol services providers
 - Continuous monitoring for vulnerabilities, malware, and intruders
 - Resolution of telecommunications and network security deficiencies
 - Design and deployment of data loss prevention technology at the TIC boundary
 - Behavioral-based analytics
 - Sharing of actionable cyber intelligence across VA and partners

- **Objective B:** *Respond rapidly to cyber threats and intrusions through timely network monitoring and detection (includes WAN, NSOC, TIC, network mapping, etc.), intelligence sharing, and advanced threat analysis techniques* – Maintaining an agile posture requires proactive capabilities informed by the results of attack pattern analysis to enhance incident response processes. To meet this objective, VA will implement the following:
 - Employment of advanced technical methods to proactively and continuously monitor VA networks
 - Enhanced incident response processes across VA through attack pattern analysis
 - VA-specific incident response playbooks and promulgation across VA and its partners

- **Objective C:** *Recover rapidly from cyber incidents through effective response, resilience, and restoration plans* – This objective will enhance readiness and resilience capabilities when incidents occur to enable users to continue to operate even under active incidents. To meet this objective, VA will implement the following:
 - Continuous monitoring to anticipate attacks and execute appropriate response and recovery capabilities
 - VA-specific incident response playbooks providing a reference guide for rapidly responding to incidents when they occur
 - Enhanced readiness, resilience, and restoration responses to cyber events

- Enablement of degraded capability modes (that is, allowing continued functions, albeit at reduced capacity) to ensure basic levels of functionality remain available while incident response protocols are executed
 - Automated failover to ensure continued availability of VA systems and data when primary ones are affected
- **Objective D: Manage risk** – This objective is to develop a better understanding of the risks to VA systems and networks through improved cyber threat identification and detection measures. To meet this objective, VA will implement the following:
 - A VA-wide security risk management framework, which includes anticipating attacks and executing appropriate response and recovery capabilities
 - Cyber event detection before they materially impact VA data and systems
 - Prioritization of risk responses based on the degree of enterprise risk
 - Accelerated adoption of lessons learned and risk mitigations
 - Managed reduction of vulnerabilities and misconfigurations
 - **Goal 2 Targets:**
 - All intrusions are responded to prior to incurring significant damage
 - Diagnostics, intelligence sharing, accelerated adoption of lessons learned and risk mitigations is continuous
 - Reduced number of critical vulnerabilities remain active in VA systems over 30 days
 - Decreased time to remediate vulnerabilities on high value assets

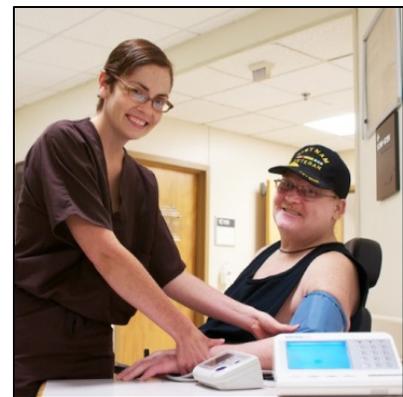


Goal 3: Protecting VA Infrastructure and Assets: Protecting VA infrastructure requires going beyond the technology and systems wholly owned and operated by VA within its facilities to include the external environments that provide potential access into VA by cyber adversaries. Public platforms such as the internet, kiosks, portals, and shared infrastructure are all potential points of vulnerability and represent assets not always under the control of

VA or the federal government. This goal will also address fortification of the interaction layers with partner organizations such as other federal agencies, shared services suppliers, commercial providers, and not-for-profit organizations empowered to act on behalf of Veterans, as well as direct access by Veterans themselves.

- **Objective A: Prioritize identification and protection of high value assets and sensitive information (local-area networks (LANs), data centers, servers, data, etc.)** – This objective identifies mission-essential networks and IT assets used to store, process, and transmit sensitive information, with added emphasis on assets delivering services to the public. To meet this objective, VA will implement the following:
 - Appropriate privacy protections
 - Inventory and situational awareness of system and information vulnerabilities for high value assets

- Continuous diagnostic monitoring on VA networks, including enterprise asset management, standard configuration monitoring, vulnerability scanning, and patching
 - Attack pattern analysis, cyber intelligence sharing across the federal government, and enhanced cybersecurity hygiene
 - Actionable intelligence for rapid, prioritized remediation of threats and exploitations against high value assets
 - Multiple layers of diverse and redundant protections (defense in depth) across people, process, technology, and operational controls
- **Objective B:** *Incorporate security and privacy protections into VA’s environment* – This objective will protect high value assets and IT systems with effective policies, processes, and tools. To meet this objective, VA will implement the following:
 - Security and privacy policies for mobile shared security, cloud, encryption, network segmentation services, digital rights management, data masking, and medical cyber devices
 - Reduction of IT infrastructure complexity through minimization of administrative privileges, strict domain separation of critical/sensitive information and information systems, and ensuring complete inventory of hardware and software components
 - Reduction of unused hardware components and software service features
 - Appropriate hardening of systems and networks with priority given to high-risk/high-impact vulnerabilities
 - Secured network enclaves with advanced techniques to detect, withstand, and recover from cyber intrusions and unauthorized data exfiltration
 - Data protection technologies such as encryption and access control
 - Common authentication, authorization, and audit services across VA
- **Objective C:** *Integrate security, application, and IT systems architectures* – This objective will harmonize current and future state architectures across business, security, applications, systems, and infrastructure domains. It integrates cybersecurity and privacy standards and design patterns to inform future systems design and ensure infrastructure protections are applied to solution development at project initiation. To meet this objective, VA will implement the following:
 - An integrated architecture framework to inform IT investment decision-making
 - Standards and protocols for medical cyber devices
 - An informed approach for securing emerging technologies (cloud, mobile, internet of things (computer and telecommunication Internet Protocol version 6 (IPv6) enabled devices such as kitchen appliances, television/video devices, and other items), etc.)
 - Enhanced configuration management processes through common security baselines (“gold images”) of VA platforms



- Integration of IT security, privacy, and medical cyber into architecture, engineering, and software development lifecycle processes
- **Goal 3 Targets:**
 - All VA assets are under active inventory management
 - Fielded solutions and shared services operate securely upon deployment
 - Decreased time to remediate vulnerabilities on high value assets

Goal 4: *Enabling Effective Operations*: Operating effectively within the cybersecurity domain requires VA to integrate its cyberspace and security capabilities and outcomes within enterprise governance, business operations, and technology architecture frameworks. This goal will improve VA cyberspace controls within the context of governance, program management, risk management, organizational alignment, roles and responsibilities, and accountabilities needed to support the envisioned future state. This goal also addresses performance management, partnerships and outreach, as well as long-range investments to ensure protections keep pace with future threats.

- **Objective A:** *Operate efficient and effective IT acquisition and procurement* – This objective enables cybersecurity practitioners to keep pace with emerging technology threats, tools and techniques devised by adversaries, as well as emerging countermeasures. To meet this objective, VA will implement the following:
 - Improved procurement processes that support quick access to emerging technology at known federal technology incubators
 - Agile and flexible IT procurement and acquisition processes to take advantage of the speed of commercial innovation
 - Standard security and privacy requirements incorporated into acquisition artifacts
 - Acquisition policies to manage supply chain risk across the entire lifecycle of products, systems, and services
- **Objective B:** *Conduct transparent and accountable operations* – This objective will result in a collective mindset in which every VA employee and contractor embraces responsibility for information security. To meet this objective, VA will implement the following:
 - A culture shift of openness, accountability, and ownership to foster enterprise-wide awareness and integration of cybersecurity requirements and practices
 - Organizational adjustments that align unit accountability with appropriate operational span of control and responsibilities
 - National network operations organization to control all VA network access and perform real-time monitoring of all VA network connections for malicious activity
- **Objective C:** *Execute integrated governance and policies across the enterprise* – This objective is to define, implement, and assure decision-making within a risk management framework driven by security and privacy requirements. To meet this objective, VA will implement the following:
 - VA enterprise-level governance processes that encompass IT security, privacy, and medical cyber

- Cybersecurity and privacy requirements considered in planning for every IT system development or acquisition effort

- **Goal 4 Targets:**

- Acquisition and procurement speed allows timely threat countermeasure response
- VA-wide visibility into cybersecurity planning, operations, and incident responses
- Cybersecurity considerations are integrated into planning, investment, and acquisition decisions for every IT system development or acquisition effort

Goal 5: *Recruiting and Retaining a Talented Cybersecurity Workforce:* Strong cybersecurity requires a workforce with talent in the multiple cybersecurity disciplines to implement and maintain the right processes, procedures, and tools. The Federal CIO’s Cybersecurity Sprint team reported their finding in the Cybersecurity Sprint Strategy and Implementation Plan for Federal Civilian Government that “the vast majority of federal agencies cite a lack of cyber and IT talent as a major barrier to the protection of information and assets.” This goal focuses on building a well-trained cyber workforce.



- **Objective A:** *Recruit, develop, and retain a world class cybersecurity workforce* – A well-functioning cybersecurity organization requires multiple disciplines to maintain pace with the growing dependence on technology for mission essential activities. This objective will enable cybersecurity professionals to continually hone skills to maintain state-of-the-art proficiencies. To meet this objective, VA will implement the following:
 - Enhancements to hiring practices including targeted recruitment to reduce time between position identification and onboarding
 - A cybersecurity workforce framework of the skills and disciplines needed to position the right people, with right skills, in place quickly

- A competency-based cybersecurity community of excellence supported by skills and theme-based development and capability maturation
 - A targeted cybersecurity retention program
 - End-to-end cybersecurity exercises of attack and defense activities (internal and external teams) to maintain proficiency
- **Objective B:** *Educate and train the VA workforce to engender a culture of cybersecurity* – This objective enables VA’s non-cybersecurity workforce to effectively operate and interact with IT systems in a secure fashion that ensures privacy of Veteran information and VA data. This will improve VA user ability to recognize and react to commonly used attack vectors, such as email phishing, click-baiting, and social engineering to reduce risks associated with these forms of attack. To meet this objective, VA will implement the following:
 - Continuous reinforcement of cybersecurity through training, education and awareness activities to improve skills, situational awareness, and understanding of operational controls
 - Initiation of certification of cybersecurity professionals
- **Objective C:** *Foster partner and supplier collaboration on shared security and privacy goals and training options* – This objective creates a shared cybersecurity culture between VA and partners. To meet this objective, VA will implement the following:
 - A program of effective long-term collaboration with industry, academia, non-profits, and other government entities to improve the collective cyberspace ecosystem
- **Goal 5 Targets:**
 - VA realizes a world-class cybersecurity workforce by 2017
 - VA’s partners and suppliers contribute to a safe and secure VA cyberspace ecosystem
 - VA’s total workforce operates consistent with cybersecurity best practices
 - Reduced time between cybersecurity position identification and hiring
 - Reduced incidents due to VA user’s improved ability to recognize and react to commonly used attack vectors, such as email phishing, click-baiting, and social engineering

PLAN EXECUTION

Implementation of the VA Enterprise Cybersecurity Strategy is accomplished by mapping each strategic goal, objective, and implementation strategy to operational domains to ensure organizational accountability and traceability. As previously noted, VA’s cybersecurity improvement effort is organized into the following domains:

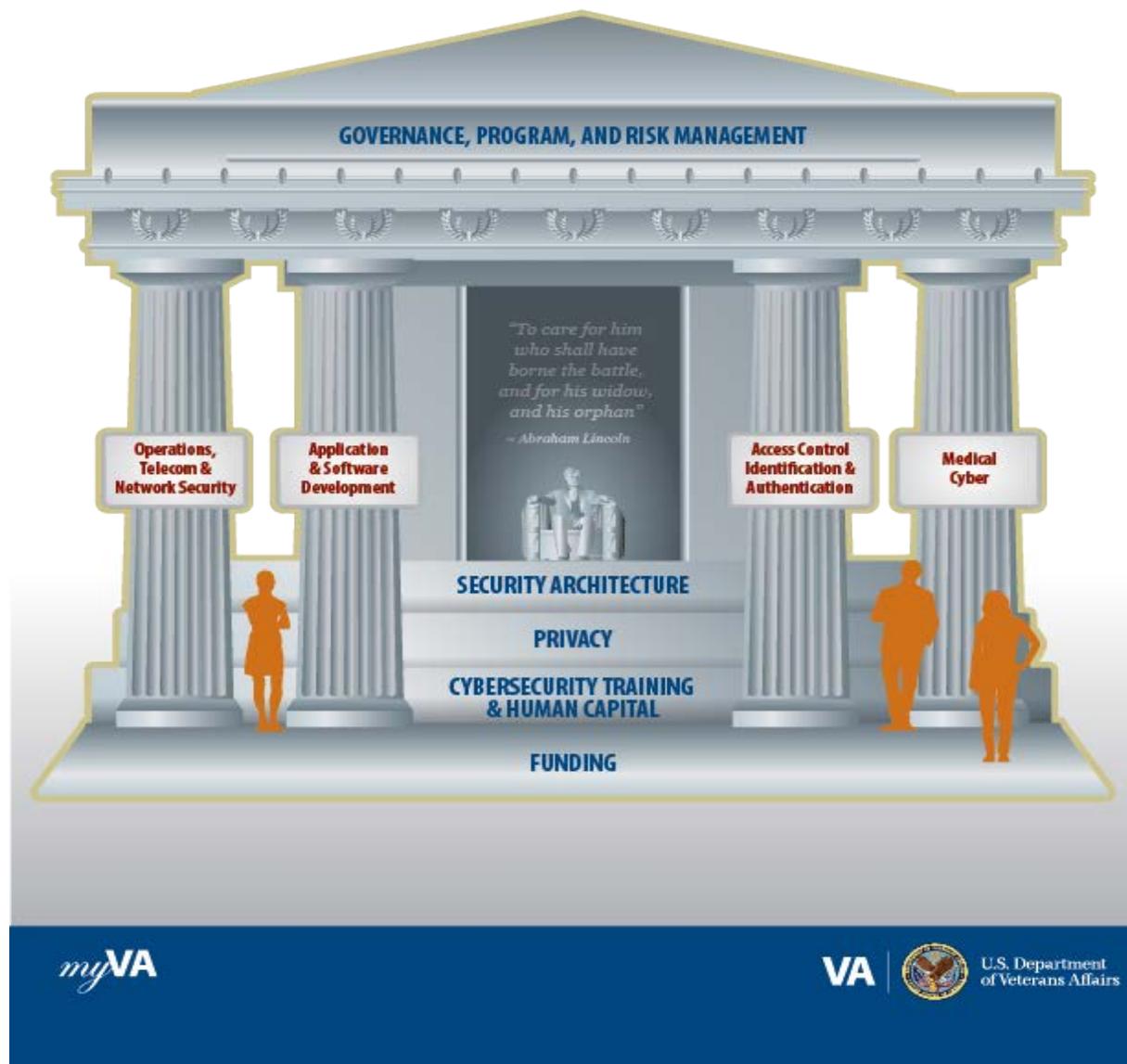
- **Governance, Program Management, and Risk Management**
- **Operations, Telecommunications (Telecom), and Network Security**
- **Security Architecture**
- **Application and Software Development**
- **Privacy**

- **Access Control, Identification (ID) and Authentication**
- **Cybersecurity Training and Human Capital**
- **Medical Cyber**

These domains are tightly coupled functions and capabilities that operate closely and are managed as integrated units. Supporting these domains is an integration function to facilitate implementation efforts that span multiple domains.

The framework for presenting VA’s associated issues is represented in the figure below. Both the domains and framework are based on security controls (National Institute of Standards and Technology (NIST) SP 800-53 Rev 4). Those domains that are cross-cutting are horizontal with funding required for all domains.

Enterprise Cybersecurity Strategy Framework



Domain Descriptions

Governance, Program Management, and Risk Management – This domain comprises the key supporting disciplines for decision-making across VA within the context of cybersecurity and privacy, including the continuous scanning of the cybersecurity landscape to proactively position VA to address emerging threats. Cybersecurity must be fully integrated into VA planning, design, and resource allocation decisions. The role of governance is to balance the needs of VA’s mission with protecting high value assets. Cybersecurity governance and program management ensure compliance with policy, rules, and standards not only during initial development of capabilities, but throughout the lifecycle. Cybersecurity governance ensures risks are understood across all aspects of the information environment and mitigation plans are developed, executed, monitored, and regularly refreshed. Cybersecurity governance addresses breaches and other incidents that affect VA’s security posture. Finally, cybersecurity governance ensures identified deficiencies are addressed and lessons learned result in enterprise-wide improvements in the guidance and processes that manage the overall environment.

Operations, Telecommunication, and Network Security – This domain comprises the key supporting disciplines for securing VA information, data, and computing assets. Security operations include people, products, and procedures to ensure data confidentiality, integrity, availability, assured delivery, and auditability of VA systems, including identity and access management, as well as network, platform, and data security. Network security includes the mechanisms to protect data and systems, and provides information assurance. Telecommunications technologies address transport, enterprise voice systems, wireless and mobile networking, and network infrastructure; included are associated standards and practices for software, hardware, networks, and telecommunication infrastructure. Collectively this domain provides security protections for any device, anywhere, at any time.

Security Architecture – This domain comprises the key supporting disciplines for developing an enterprise information security architecture (EISA). EISA is the practice of applying a comprehensive method for describing a current and/or future structure and behavior of an organization's security processes, information security systems, personnel, and organizational sub-units. This will ensure VA’s alignment with its core security goals and strategic direction. Although often associated strictly with information technology it also supports business optimization. This domain includes the design and engineering skills needed to fully integrate security into VA’s overall business, applications, and IT systems architecture.

Application and Software Development – This domain comprises the disciplines needed to ensure applications used during the provision of services to Veterans utilize the most secure practices for data storage, access, manipulation, and transmission. Encompassed is the entire software lifecycle, from requirements identification, design, development, testing, deployment, training, patch management, and configuration management through end-of-life system retirement. Software assurance, that is, the level of confidence VA software is free of vulnerabilities or defects that could lead to vulnerabilities, is a critical concern for the Application and Software Development Security Domain. Included are the cybersecurity design patterns, standards, and processes for software built by VA, vendors, and commercial off the shelf software included in the VA’s suite of systems.

Privacy – This domain addresses policy and legislatively driven requirements for PII and PHI. While Federal statutes, regulations, executive orders, policies, procedures, and guidance mandate privacy efforts, VA is challenged to implement an effective and efficient enterprise privacy strategy across VA’s Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), National Cemetery Administration (NCA), and private health care providers. This domain is focused on implementing the “Best Practices: Elements of a Federal Privacy Program,” published by the Federal CIO Privacy Committee. The strategic privacy planning framework consists of seven key elements: Leadership; Privacy Risk Management and Compliance; Information Security; Incident Response; Notice and Redress; Privacy Training and Awareness; and Accountability. This framework is key to implementing PII and PHI privacy requirements.

Access Control, Identification and Authentication – This domain comprises the disciplines needed to secure the environment and provide the mechanisms to mitigate vulnerabilities, reduce the likelihood and impact of security incidents, and eliminate threat vectors. Access control (AC) is a combination of authentication and authorization processes that allow access to VA networks, hardware computing devices, and applications to ensure compliance with directives including Homeland Security Presidential Directive 12 (HSPD-12) and the Federal Information Processing Standards (FIPS) 201 guidelines. Identification and authentication (IA) is the process of verifying the identity of a user, process, or device through the use of specific credentials such as passwords, tokens, and biometrics as a prerequisite for granting access to system resources. Together AC and IA are required for securing PII and protected health information (PHI) by limiting system access to authorized users, processes, and devices.

Cybersecurity Training and Human Capital – This domain comprises the hiring practices and skills maturation needed to create a workforce steeped in a culture of cybersecurity to proactively protect all data and information of the Veterans we serve. Needed are professionals with requisite skills to maintain pace with the security and privacy implications associated with the growing dependence on technology for VA’s essential activities. To achieve the culture of cybersecurity, this domain includes partnering with other agencies, academia, industry, and certification bodies to create an enriched environment in which state-of-the-art practices and proficiencies can be honed and maintained.

Medical Cyber – This domain focuses on medical devices not traditionally considered IT that can be networked or accessed electronically. In the past, medical devices were standalone instruments that interacted only with the patient. Today, incorporation of information and communications technology has transformed medical devices by enabling their clinical functions and data to be digitized, remotely accessed and managed, made interoperable with other devices and systems, and integrated into the healthcare business IT environment. Just like servers that collect and transmit PII and PHI, these IT-enabled and networked medical devices must be protected from exploitation and from becoming operable vectors for cyberattacks. While this domain will focus initially on medical devices, over time it will expand to encompass all “cyber physical” systems with similar electronic characteristics. This includes devices typically associated with physical plants such as industrial control and elevator systems, as well as the Internet of things, that is, non-traditional devices that are becoming increasingly sophisticated in their incorporation of IT, software applications, telecommunication, and networking capabilities, such as kitchen appliances, television/video devices, and other items commonly found in VA facilities.

Key Implementation Considerations

Timeline and Sequencing

Implementation strategies will deliver capabilities and support operations critical to achieving the higher level goals, targets, and objectives. Implementation strategies identified in the VA Enterprise Cybersecurity Strategy are supported by actions and implementation plans in each domain report.

Each implementation strategy will have a domain to lead the effort while other domains contribute with additional implementation plans that reflect their contribution to success. These implementation plans are prioritized across three time horizons to effectively balance the following factors:

- Impact and importance (e.g., remediation of existing material weaknesses)
- Organizational capacity
- Logical interdependencies that drive precedence
- Incremental staging to deliver early benefit realization while progressively moving towards full impact realization over a longer time horizon.

The first time horizon focuses on near-term high-priority efforts that deliver incremental progress towards outcomes within zero to six months. The second time horizon focuses on mid-term initiatives that deliver results within seven-to-twelve months. The third time horizon focuses on long-term initiatives that deliver results in a timeframe of thirteen months or longer. In many cases these efforts start within the near-term time horizon, however results will not be realized until a later timeframe.

Progress/Performance Reviews

OI&T will monitor progress toward implementation plan completion and outcome attainment by domain teams, accountable OI&T organizations, and VA mission functions responsible for delivering services to Veterans. These reviews will provide governance entities with insightful analysis and recommendations to adapt the strategy and/or implementation plans for efficiency and effectiveness. The reviews will track schedule and budget execution; address current operational situations facing VA; assess completeness of requirements delivery and attainment of goals, targets, and objectives. This will inform course corrections that could encompass scope, schedule, resources, risk responses, compliance/enforcement actions, policy, operations, and future investments.

Risks

Implementing the VA Enterprise Cybersecurity Strategy is not an endeavor free of risk. It is a fundamental premise that even given unlimited resources, time, and expertise, no agency or organization will eliminate 100 percent of every possible threat or risk. Therefore, adopting strategies to reduce or mitigate VA's risk profile is a critical focus of the implementation plan, to include:

- Establishing a transparent decision-making and governance structure that ensures an integrated and synchronized approach
- Prioritizing those security measures that reduce threats and vulnerabilities to VA systems and data to make the best possible use of resources
- Fostering interagency and inter-departmental partnerships to leverage existing and emerging capabilities
- Continuously monitoring and assessing the effectiveness of risk mitigation and risk reduction actions to manage vulnerabilities.

CONCLUSION

VA delivers its mission to serve Veterans in an ever-changing landscape, continually adapting to the emergence of innovative technologies. VA's Enterprise Cybersecurity Strategy is a major step forward in VA's commitment to safeguarding Veteran information and VA data within a complex environment. The strategy establishes an ambitious yet carefully crafted approach to cybersecurity and privacy protections that enable VA to execute its mission of providing quality healthcare, benefits, and services to Veterans while delivering on our promise to keep Veteran information and VA data safe and secure.

Recognizing our society is in a constant state of technological change, the implementation plan is dynamic, designed to be flexible and agile in addressing future and emerging needs while effectively tackling present day requirements in a sustainable and responsive manner. The plan takes an assertive posture on adopting the latest Federal Cybersecurity Strategic Plan tenets for Federal civilian agencies. Each of the strategy's goals and objectives are decomposed into outcome-driven actions, and VA will manage progress towards each goal and objective through discrete performance measures. While technology is a prominent feature of the plan, to be truly transformative, it must address actions necessary to make the organization more transparent, accountable, innovative, and team-oriented.

The strategy also reflects VA's commitment to the President's vision for a Federal Cyber Strategy and the VA Secretary's MyVA transformation. VA firmly believes the core principles of transparency, communication, and collaboration are critical to the strategy's success. As such, the strategy takes a broad approach involving local, state, Federal, and private sector partners, as well as the American public. Integrating the best our partners have to offer with feedback from those we serve will allow us to prioritize our investments and efforts toward achieving our desired outcomes. Throughout this transformation, our number one priority remains the Veteran. OI&T will ensure a safe and secure environment for all Veteran information and VA data.