Department of Veterans Affairs

Cybersecurity Strategy

VA

U.S. Department of Veterans Affairs

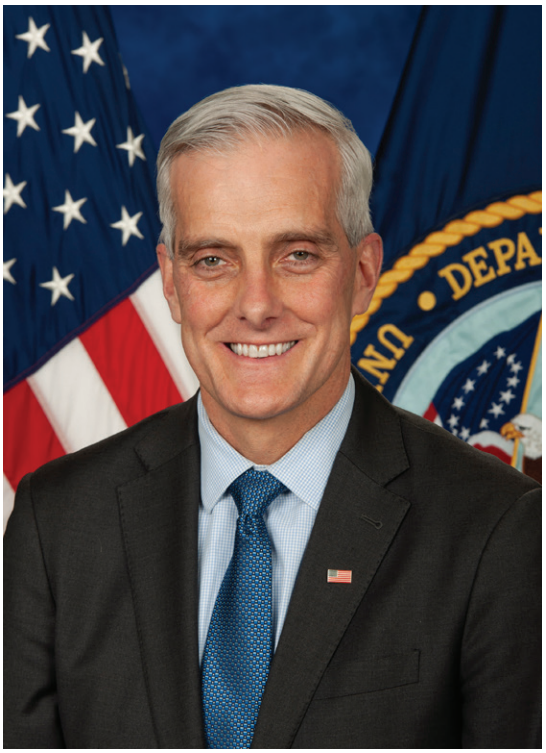
Office of Information and Technology

References herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise do not necessarily constitute or imply endorsement, recommendation, or favoring by the United States Government and shall not be used for advertising or product endorsement purposes.

This document includes links to other 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.

Table of Contents

Message from the Secretary



At VA, it is our mission to serve Veterans, their families, survivors, and caregivers as they have served our Nation—and cybersecurity is a critical part of that effort.

Whenever VA beneficiaries come to us for the care and benefits they've earned, they need to be able to trust us to secure their information and protect their privacy. This cybersecurity strategy will help VA keep that promise by addressing the challenges of today and adapting to the technologies and threats of tomorrow. It will also make VA more agile and innovative, allowing us to improve on what matters most: access and outcomes for those we serve.

Cybersecurity is a team effort, especially given the rapid rate of technological advancements across VA. That means all VA employees and contractors must do our parts to safeguard sensitive and private information, practice accountability and transparency, and remain hypervigilant of cyber threats. This strategy will help all of VA execute that mission, charting a course for success at the individual and enterprise levels.

I look forward to working with our partners in Congress and all relevant stakeholders to put this plan into action, and—in doing so—better fulfilling our sacred obligation to care for "those who shall have borne the battle," their families, survivors, and caregivers.

Denis McDonough
Secretary of Veterans Affairs

Introduction

Although the U.S. Department of Veterans Affairs was officially established as a Cabinet-level agency, on March 15, 1989, the commitment to our Nations' Veterans has been present since the early founding of our Nation. As the Nation has grown, so too have the expectations of the types of support and level of services that encompass that commitment. VA maintains a lifetime relationship with millions of Veterans and their families.

Technology has greatly improved the quality of life for all citizens. Likewise, technology has improved the level of care and the accessibility of services to Veterans and other beneficiaries. Today, VA is the largest integrated health care system in the United States, with health care facilities and outpatient clinics across the country. VA also provides a series of non-healthcare benefits including disability compensation, vocational rehabilitation, education assistance, home loans, and life insurance, and provides burial and memorial benefits to eligible Veterans and family members at 135 National cemeteries.

As we leverage technology for the betterment of VA's service offerings, we must also bear the responsibility in protecting the Department's critical information resources. The Veteran experience includes the safeguarding of their information and the protection of the systems that store, process, and transmit data. A compromise could lead to fraudulent activities, exposure of Veteran's personal information, or the corruption of critical data. More importantly, poor cybersecurity practices will erode the Veteran's confidence in VA.

The underlying message is clear: cybersecurity is essential to the success of VA's mission.

The following five Strategic Goals outline the Department's focus on maintaining a robust and resilient technology environment that advances VA's mission:

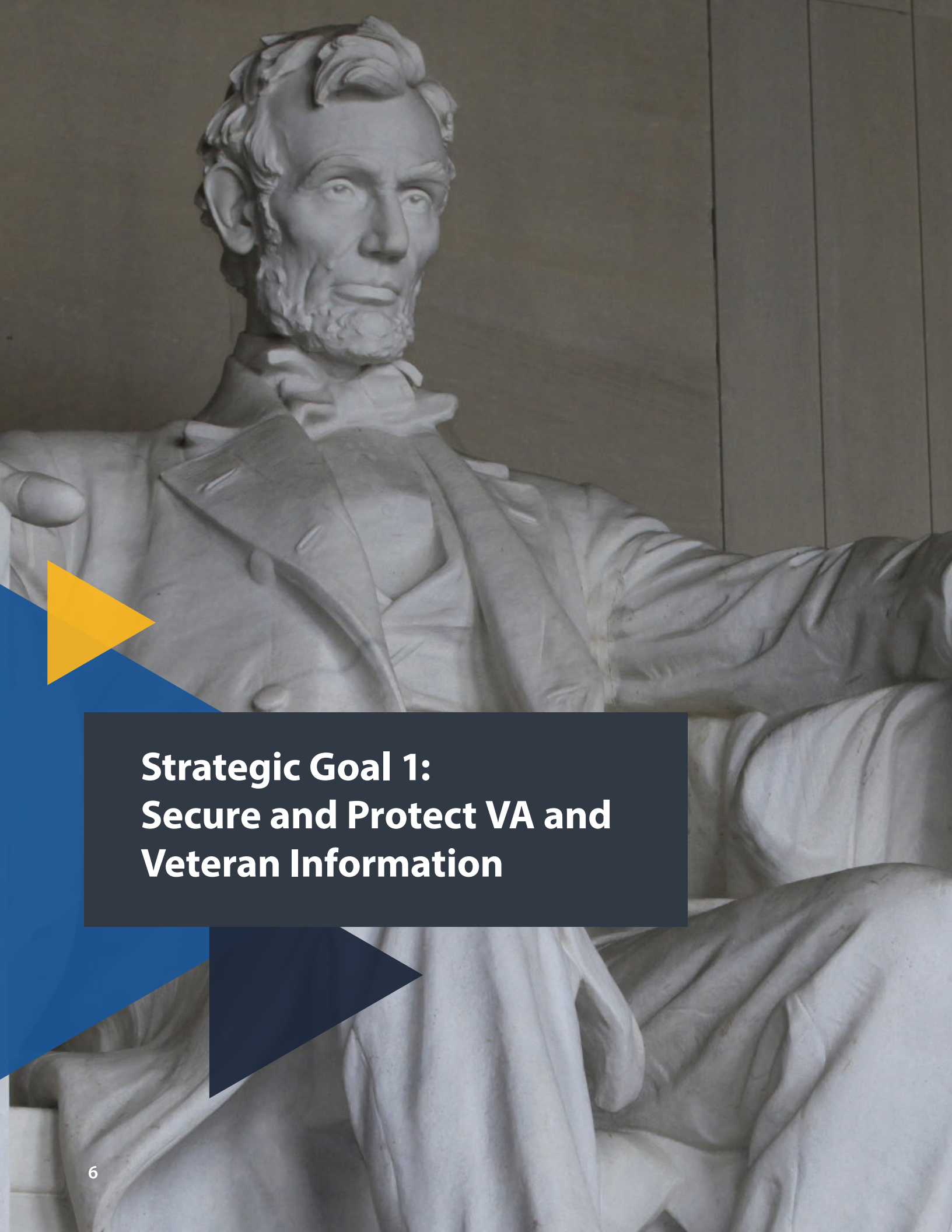
- Secure and protect VA and Veteran information
- Protect information systems and assets
- Leverage innovation to strengthen cybersecurity
- Enhance cybersecurity through partnerships and information sharing
- Empower VA mission through cybersecurity risk management

This strategy aligns to and enables the FY18-24 VA Strategic Plan and takes into consideration existing and new Federal cybersecurity requirements, technological advancements, innovations, and world events that have evolved the way VA delivers services. It also factors in new and innovative ways to protect against today's most sophisticated cybersecurity threats. Central to this strategy are the core values America's Veterans have taught us by example: Integrity, Commitment, Advocacy, Respect, and Excellence (I CARE). These core values guide all our interactions as we implement VA's Cybersecurity Strategy.

VA FY18-24 Strategic Plan	VA FY22-26 Cybersecurity Strategy				
	Secure And Protect VA and Veteran Information	Protect Information Systems and Assets	Leveraging Innovation to Strengthen Cybersecurity	Enhance Cybersecurity Through Partnerships and Information Sharing	Empower Mission Through Cybersecurity Risk Management
Veterans choose VA for easy access, greater choice, and clear information to make informed decisions.	☆	☆	☆	☆	★
Veterans receive timely and integrated care and support that emphasizes their well-being and independence throughout their life journey	☆	☆	☆	☆	★
Veterans trust VA to be consistently accountable and transparent	★	☆	☆	★	☆
VA will modernize systems and focus resources more efficiently to be competitive and to provide world class capabilities to Veterans and its employees	☆	★	★	☆	☆

This strategy guides efforts to deliver cybersecurity services in a measurable and effective way, that enables the protection and resilience of VA's most critical business functions and assets. The associated objectives and actions of this strategy are accomplished through collaborative, engaged, and informed stakeholder partnerships where mission success is realized through stakeholder accountability. The implementation of this strategy will be closely governed and measured for success, remaining agile to the evolving needs of VA's mission.

The VA Office of Information Security (OIS) is responsible for overseeing the Department's Cybersecurity Program as prescribed by the Federal Information Security Modernization Act of 2014 (FISMA) 2014 (44 USC Section 3554). OIS will manage the Cybersecurity Program (with Departmental approval through the Chief Information Officer (CIO)) to address the Strategic Goals outlined in this Cybersecurity Strategy.



Strategic Goal 1: Secure and Protect VA and Veteran Information

Information is at the heart of VA's mission. VA is the custodian of information on millions of Veterans, their families, and caregivers. The Department also maintains an extensive amount of information that supports mission operations, research and development, and business interactions. With this wealth of information, the Department provides timely access to benefits and services, advanced healthcare and medical research, and leverages services offered by the private sector. In VA, information is an essential Departmental asset.

As custodians and stewards of sensitive data, VA is committed to preserving the trust of Veterans, partners, and the public. Veterans, their families, and caregivers have entrusted VA to manage and protect their personal health records and financial information with their interest in mind. Likewise, VA's public and private partners trust that VA manages and protects information under our control. Our mission is stronger with their confidence, and we will maintain that trust through sound judgment and care.

The Department will be proactive in protecting the confidentiality, integrity, and availability of information to meet today's mission and for the future. Veteran data and VA information are of great interest to adversaries who seek financial gain, market influence, or other types of exploitation. Loss or compromise of information can place Veterans and our mission at risk. Therefore, the Department is committed to leveraging Federal standards and best business practices to protect information as a Departmental asset throughout its lifecycle.

VA secures and monitors information repositories. Similarly, we protect the transmission of electronic data shared between systems, sites, or business partners. Protecting these information exchanges is critical to expanding the success of key programs such as telehealth.

- 1.1: Identify and tag sensitive data
  Identifying VA controlled data that requires protection from unauthorized use or access
- 1.2: Protect data at rest
  Encrypting data stored on hardware and network assets
- 1.3: Protect data in transit
  Securing the means, ports, and protocols used in data transmission
- 1.4: Prevent data loss
  Detecting and preventing unauthorized access, spillage, or exfiltration of data through dataflow monitoring and management

Strategic Goal 2: Protect Information Systems and Assets

Advancements in technology have greatly improved the quality, access, and timeliness of VA services and support. We live in a world of online ordering and 24-hour delivery, where we can monitor our physical state in real-time, and pay bills and complete banking transactions easily from our phone. Veterans, their families, and caregivers expect that same level of access and convenience in their engagement with VA.

VA depends upon secure information systems to enhance the mission. From remote mobile devices to secure connections between VA facilities around the world, VA depends on technology to provide the tools and infrastructure to manage information and promote collaboration. We continue to use technology to manage medical devices, control facility access and environment, and manage personnel. Our interactions with Veterans also leverage technologies through virtual interfaces and augmented service delivery.

Therefore, the protection of VA systems is essential to mission delivery. In protecting information systems and assets, we assist VA business owners in providing effective and timely services. Secure environments provide the platform for information exchange, technology development, and innovation. It also decreases the threat of attack while providing the resiliency to continue operations in the event of an incident.

To that end, we must engage in sound security practices that protect our information resources. This includes assuring cybersecurity throughout the network and in the deployment of tools, applications, and equipment used to store and access data. It also means taking the necessary safeguards in authenticating, authorizing, and allowing access to information resources.

The Department will continue to incorporate technologies for greater empowerment of Veterans and staff while protecting information system resources toward mission success today and in the future.

The following objectives support the protection of information systems and assets:

- 2.1: Maintain full visibility and accountability of all hardware and software assets
  Manage the configuration and provisioning of VA IT hardware and software assets
- 2.2: Maintain full visibility and accountability for all VA information systems
  Ensure information systems are known and managed within their authorized environments
- 2.3: Enhance and safeguard authorized system access
  Authenticate users and control their access based on assigned roles and responsibilities
- 2.4: Proactively secure VA networks
  Apply standards and best practices to prevent unauthorized access and improve the detection of malicious activities
- 2.5: Promote resilience through effective response and recovery
  Minimize impact to business operations and continuity in the event of a compromise, data loss, or breach

Strategic Goal 3: Leverage Innovation to Strengthen Cybersecurity

Innovation has produced many advancements in technology, improving VA's ability to provide services to Veterans, enriching the care they receive, and strengthening the posture and resilience of our IT Infrastructure. Cybersecurity and innovation must work in concert in a risk-balanced, forward-leaning approach for mission success.

Veterans, their families, and caregivers are becoming increasingly tech savvy and they expect VA to be as well. We must be able to provide the same virtual experience and ease of access offered by the private sector. For instance, advancements in mobile devices, smart technology, and operational technology (OT) are changing how customers engage with service providers and how technology interacts with the physical world. The Department can leverage these types of technical advancements in medicine, facility management, and customer engagement to improve our service offerings and more effectively manage our resources. However, like our commercial counterparts, we must balance ease of connection with necessity of access and convenience balanced with confidence of protection.

Technological innovation has allowed the Department to be more agile in delivering IT and cybersecurity services. For instance, advancements in machine learning and artificial intelligence have greatly improved the ability to anticipate outages and detect anomalous behaviors in an ever-growing pool of IT performance data. By valuing innovation through advanced technologies such as quantum computing and block chain, the Department is poised to capitalize on new technologies to bolster service delivery and address evolving risks to networks, information systems, and VA data.

Technology change can be intimidating. Yet every new generation of advancement promises better services, more options for care, convenience, and new challenges. As we move into the future, this strategy positions VA to leverage the benefits of innovation to deliver world-class services that fully incorporate cybersecurity protections.

The following objectives support leveraging innovation to strengthen cybersecurity:

- 3.1: Streamline processes through adopting innovative solutions and capabilities
  Finding new technologies to address challenges and improve processes
- 3.2: Embed cybersecurity in systems engineering and acquisition processes
  Ensure that IT application, system, and network solutions include cybersecurity in design, engineering and acquisition
- 3.3: Adopt innovative cybersecurity solutions
  Leverage technology to enhance the Department's cybersecurity capabilities
- 3.4: Empower VA workforce to integrate cybersecurity in daily operations
  Recognizing that all VA employees play a role in cybersecurity and they are the Department's first line of defense

Strategic Goal 4: Enhance Cybersecurity Through Partnerships and Information Sharing

We enhance cybersecurity when we work together as a community. This means we strengthen our capabilities when we work with internal and external partners. We gain knowledge by sharing our perspectives, strategies, solutioning experience, and threat information. By leveraging each other's work and jointly engaging to address common issues, we provide a unified and more difficult attack surface for our adversaries. Through trusted partnerships we improve the Department's mission, contribute to the Federal government cybersecurity efforts, and strengthen confidence with our private partners.

Collectively, all VA efforts deliver the Department's mission and define the Veteran's experience. It is imperative to the mission that VA's secure computing environment enhances the delivery of service while protecting VA's information resources. VA depends on internal partnerships to provide awareness of changes in technology and cybersecurity risks. This awareness aids the Department in identifying and mitigating cybersecurity concerns in a mutually beneficial and risk-managed approach.

The Department also values its external partners and benefits from the knowledge and experience of others. Government organizations and private industry all face cybersecurity risks like those facing VA. Through partnerships with others, we learn what threats they are encountering, and we share our experiences. Other organizations share the techniques they have successfully used in addressing cybersecurity risks, allowing us to adopt proven solutions. Similarly, we can avoid solutions that other organizations have tried without success. Information sharing relationships, partnerships, and collaboration with other organizations through which we share our cybersecurity program's successes and learn about the successes of others not only improves our cybersecurity but also improves the cybersecurity of our partners, their partners, and the Nation.

Ultimately, trusted partnerships within VA and with external organizations provide the knowledge and experiences needed to make risk-based and threat-informed decisions. Partnerships also elevate the commitment to and value of cybersecurity in strengthening VA's mission and enabling resilient business operations.

The following objectives support enhancing cybersecurity through partnerships and information sharing:

- 4.1: Elevate cybersecurity as a mission and business enabler
  Bringing value to the mission and business
- 4.2: Remove barriers to sharing threat information
  Understanding that information sharing elevates the cybersecurity posture of all
- 4.3: Enhance internal partnerships and cybersecurity coordination
  Providing cybersecurity assistance and solutions that are actionable and with our partner's interest in mind
- 4.4: Promote mutually beneficial external cybersecurity partnerships
  Recognize and leverage partnerships with other Federal Agencies and the private sector for mutual support and cybersecurity awareness

Strategic Goal 5: Empower Mission Through Cybersecurity Risk Management

Over the last decade, the Department has become increasingly dependent on secure technology to operate and meet mission objectives. First and foremost, technology has greatly improved accessibility to benefits, delivery of services, and the quality of care to Veterans, their families, and caregivers. It has provided the means to conduct advanced research in partnership with industry, universities, and National laboratories. Additionally, technology provides essential connectivity, resource management, and infrastructure in support of the Department's growing physical and virtual landscape.

Cybersecurity has become a business enabler while also remaining a protector of information resources. Securing VA's information and information systems is a continual challenge due to emerging threats, the incorporation of new technology, and evolving mission requirements. Adding to the challenge is the complexity of the network, legacy systems, and competing operational priorities. However, cybersecurity must remain centered toward secure mission support today, while protecting information resources for the future.

To empower our mission, risk management must be at the heart of our cybersecurity strategy. We should not take unnecessary risks for the sake of the mission nor should we miss opportunities purely to meet compliance targets. This is especially true regarding implementing technology and addressing cybersecurity risks. New threats and vulnerabilities are an expected constant in cybersecurity. We must recognize where they occur and take a balanced, proactive, and risk-based approach in addressing them.

Likewise, the Department must also consider the protection of information resources as an essential element in delivering services and benefits. In protecting our resources today, we assure their availability in the future and reduce the cost associated with a loss of information or other assets. Decision makers must consider technical cost and cyber risk in the decision calculation. Stakeholders and decision makers must work together to make informed risk-based decisions based on clear and timely analysis and guidance.

This cybersecurity strategy supports and protects the Department's mission, decisional authorities, and information resources. Cybersecurity risk management involves properly assessing the risk and making an informed decision on how to address the threat or vulnerability. The Department cannot afford to blindly accept the risk or ignore the risk completely. We must address discoveries in a transparent, risk-based, and accountable manner.

The following objectives empower mission through cybersecurity risk management:

- 5.1: Reduce exposure in high-risk areas
  Address known vulnerabilities and risks that could have a major impact on the Department's mission
- 5.2: Strengthen trust in VA's cybersecurity program
  Refine and strengthen the Department's cybersecurity program through transparency and mission alignment
- 5.3: Promote informed cybersecurity risk management decisions
  Foster a culture of risk-aware planning, thinking and decision-making

Conclusion

Veterans, their families, and their caregivers deserve world-class benefits and services. In providing this support VA must leverage technology to improve access, enhance quality of care, and fulfill our commitments to those who have proudly served our country.

With advances in technology comes a responsibility to ensure the protection of sensitive information necessary to execute the Department's mission. Providing this protection is a Department-wide responsibility.

VA's FY22-FY26 Cybersecurity strategy is a framework that supports The Department's mission, and serves as the central focus for setting cybersecurity priorities. The strategy sets a foundation to meet today's challenges while supporting agile development and incorporate new technology and innovation in a secure manner.

This cybersecurity strategy is a blueprint that requires commitment, coordination, and accountability across the entire Department. We all play a critical role in the execution of this strategic vision and remain steadfast in our support of our Nation's Veterans.

U.S. Department of Veterans Affairs

Office of Information and Technology

www.oit.va.gov