VA Enterprise Design Patterns
Information Technology (IT) Service Management

Vulnerability Management

Office of Technology Strategies (TS)
Office of Information and Technology (OIT)

Version 1.0
Date Issued: February 2018

Approval Coordination

Deeneen U Akeo 622220

Digitally signed by Deeneen U Akeo 622220
Date: 2018.02.08 20:57:10 -05'00'

Deeneen Akeo
Director, Architecture & Engineering, EPMO Demand Management

Everett, John P.

Digitally signed by Everett, John P.
Date: 2018.02.14 13:28:15 -05'00'

John Everett
Executive Director, EPMO Demand Management

Revision History

Version	Date	Organization	Notes
1.0	December 2017	ASD TS	Final version for TS leadership approval and signature, including all applicable updates addressing stakeholder feedback and Section 508 compliance

CONTENTS

QUICK JUMP

Select an icon to skip to a section.

Current Capabilities
Future Capabilities
Use Cases
One-VA Technical Reference Model
The Veteran-Focused Integration Process
Enterprise Design Pattern Scope

1 INTRODUCTION

The Department of Veterans Affairs (VA) must store, protect, and provide appropriate access to Personally Identifiable Information (PII), Protected Health Information (PHI), and Sensitive Personal Information (SPI) for approximately 21.8 million Veterans and their dependents; and VA must secure internal sensitive data. With awareness that some of the most significant data breaches to date have involved vulnerabilities that could have been prevented, including the Equifax[1] and Office of Personnel Management (OPM)[2] incidents, VA is committed to reducing the risk of data compromise. VA must identify the requirements to close security gaps and incorporate security policy compliance as part of a comprehensive VA Vulnerability Management (VM) program. VM is the process of identifying, classifying, and mitigating vulnerabilities – weaknesses that reduce the protection of the integrity, availability, authenticity, non-repudiation, and confidentiality of user data. VM is dependent upon configuration management, change management, asset management, and network security to effectively manage vulnerabilities.

The VA Office of Inspector General (OIG) has repeatedly cited recommendations[3] over a period of several years in an effort to improve the VM program at VA. This Enterprise Design Pattern

[1] https://www.scmagazine.com/apache-struts-vulnerability-led-to-earlier-breach-at-equifax/article/689863/

[2] https://www.darkreading.com/vulnerabilities---threats/opm-breach-exposes-agencys-systemic-security-woes/d/d-id/1320794

[3] https://www.va.gov/oig/pubs/VAOIG-16-01949-248.pdf

(EDP) will provide requirements for implementing an enterprise-wide VM program that is based on VA compliance and industry best practices.

1.1 Business Problem

Assessments of VM solutions and processes at VA have indicated a need for a more effective, centralized VM program to address security deficiencies throughout the enterprise.

The following limitations have been identified in the current VM program:

- Lack of a unified enterprise patch management strategy
- A lengthy vulnerability discovery-to-mitigation timeline
- Lack of automation within the VM process
- Lack of effective vulnerability prioritization
- Lack of consistent configuration baselines, impeding patch management
- Lack of a standard strategy for unsupported software that is still required to support business operations

1.2 Business Need

Federal Information Security Management Act (FISMA) compliance, agency policy, and enterprise strategy are drivers for the following business needs at VA (Please see Appendix D for specific policies):

- A mature VM program that can resolve the FISMA audit findings
- Prioritization strategy, with enough granularity to account for the highest areas of risk when resources are limited
- An efficient VM program that minimizes risk exposure, while supporting service delivery
- A single strategy for the alignment of tools to the VM program; including removing tool overlap and resulting data conflicts, and integration with the Continuous Diagnostic and Mitigation (CDM) program
- A timely and reliable reporting that is based on authoritative data sources
- An authoritative source of IP address to system and system owner mapping

1.3 Business Case

VM is integral to risk management. Table 1 provides the business benefits for improving VM within the enterprise.

Table 1: Business Benefits

Business Benefits	Description
VM Program Governance	A governance program will remove the roadblocks impeding the current process, and will be granted authority over the service and measure its success.
Unified Strategy for Enterprise Vulnerability Management	A single strategy to align all processes and solutions to VM program goals; and adoption of an enterprise strategy, such as shared services; acts to increase compliance and reduce redundancy; a unified strategy will create a more efficient and effective VM program.
Federal and VA Compliance	A robust VM program supports compliance with FISMA, the National Institute of Standards and Technology (NIST), VA policy, and other federal requirements to prevent unfavorable audit findings.
Increased Security/Decreased Risk Exposure	A centralized VM program will decrease risk to business services by reducing vulnerabilities associated with other capabilities, such as configuration management and network security.
Accurate and Timely Business Intelligence	Accurate reporting that is based on authoritative data sources and solutions aligned to program requirements will increase visibility, availability of information for use in risk management, and federal compliance reporting.

1.4 Approach

This EDP provides a vendor-agnostic approach to VM to support the discovery, prioritization, and remediation of vulnerabilities across the enterprise. The document will assist VA project teams, IT investment decision-makers, the Strategic Technology Alignment Team (STAT), and other stakeholders to identify issues associated with resolving FISMA audit and material weakness findings; and to make recommendations for program improvement. The EDP approach includes the following:

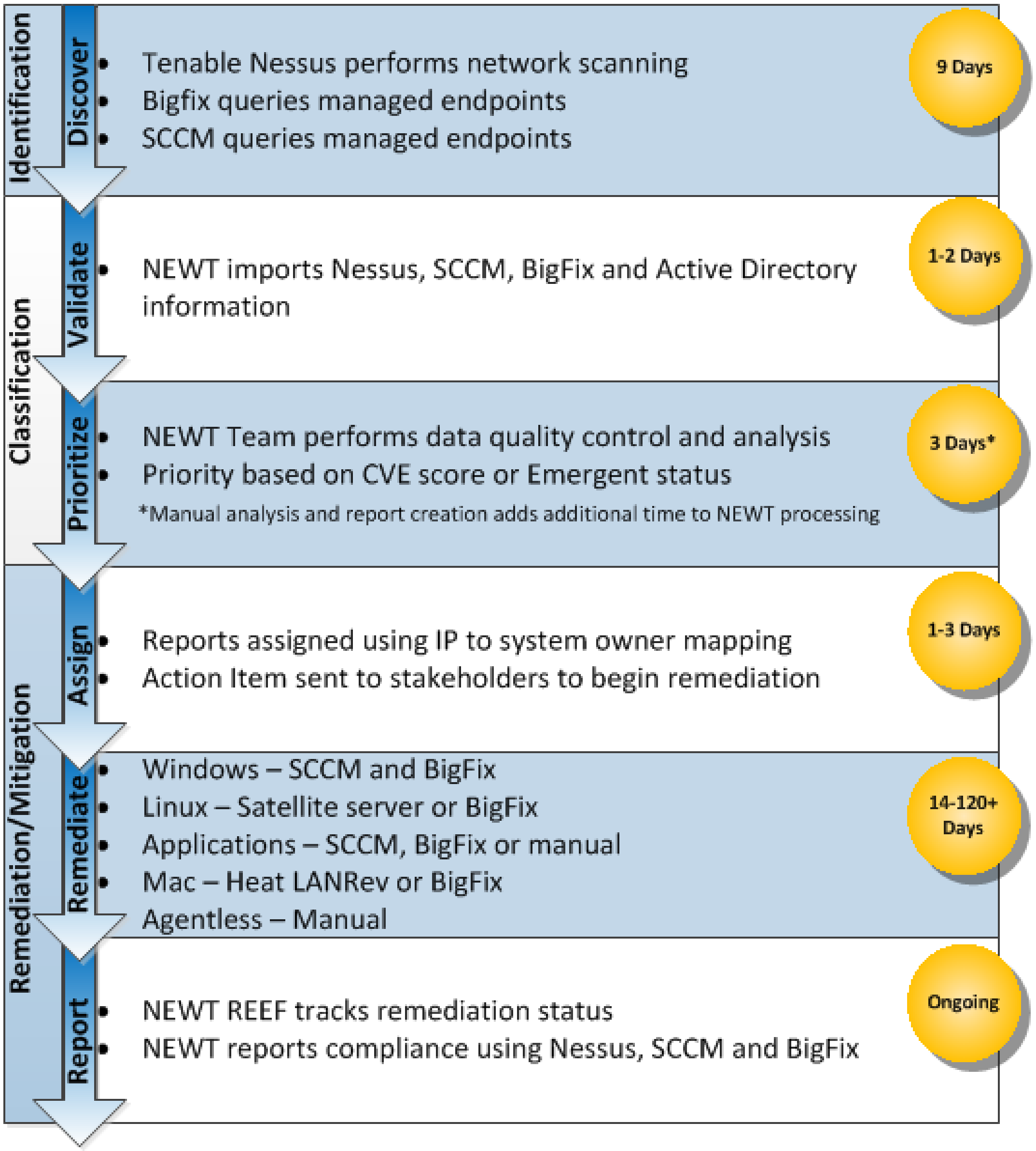
- Review existing capabilities and their limitations
- Analyze existing policy and governance
- Provide parameters for improving VM at VA

2 CURRENT CAPABILITIES AND LIMITATIONS

The VA Office of Information and Technology (OIT) includes enterprise-wide services for VM that makes use of a number of scanning tools to execute processes within the following phases:

- **Identification** - Identify endpoints and devices attached to the VA network and analyze them for security deficiencies.
- **Classification** – Validate security deficiencies and map to the Common Vulnerabilities and Weaknesses (CVE), Common Weakness Enumeration (CWE), or other types of classifications.
- **Remediation** – Vulnerability classification information and other risk data is used to prioritize and execute remediation activities.
- **Mitigation** – For vulnerabilities that cannot be remediated, mitigation is performed to lower risk to acceptable levels.

While VM tools are effective in their primary functionalities, VA has acquired multiple tools to provide enterprise coverage, taking on functions that sometimes overlap. The figure below provides a high-level view of the current capabilities within the VM process and the estimated time (in days) to execute each phase required to identify and remediate vulnerabilities.



- Tenable Nessus performs network scanning
- Bigfix queries managed endpoints
- SCCM queries managed endpoints

- NEWT imports Nessus, SCCM, BigFix and Active Directory information

- NEWT Team performs data quality control and analysis
- Priority based on CVE score or Emergent status

*Manual analysis and report creation adds additional time to NEWT processing

- Reports assigned using IP to system owner mapping
- Action Item sent to stakeholders to begin remediation

- Windows – SCCM and BigFix
- Linux – Satellite server or BigFix
- Applications – SCCM, BigFix or manual
- Mac – Heat LANRev or BigFix
- Agentless – Manual

- NEWT REEF tracks remediation status
- NEWT reports compliance using Nessus, SCCM and BigFix

FIGURE 1: CURRENT VM PROCESS MAPPING

2.1 Identification

VA currently deploys Tenable Nessus as its primary tool for network scanning for vulnerability identification. Nessus is centrally managed. Nessus uses a network of distributed virtual scanners to perform agentless security scans of devices that are attached to the VA network. The Nessus scans check compliance with standards, such as the United States Government Configuration Baseline (USGCB) and the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). The Nessus scans also check for missing patches, insecure system configuration settings, and the use of default or weak credentials. Although vulnerability identification is steadily improving, current challenges include the following:

- There is not an authoritative data source or enterprise governance over the distribution of Internet Protocol (IP) addresses. Crowdsourcing is used to self-report ownership of IP addresses to be scanned.
- A large volume of IP addresses require evaluation. This currently takes approximately nine (9) days to complete. Enterprise scanning is performed on a 30 day cycle.
- Vulnerability identification is only performed using agentless scanning, adding to network overhead. Network latency can delay operations for facilities that are connected over slow links and cause the Nessus scan job to fail.
- Credentials are not available for all devices, decreasing the accuracy of some scan results.
- Some stakeholders refer to the Nessus System Center Configuration Manager (SCCM) and IBM BigFix data, which may produce conflicting results. Guidance over the normalization and use of these different data sources is not clearly defined. Automation is not applied for analysis.
- Integration of CDM solutions is in progress.

2.2 Classification

The approximately one million IP addresses that are scanned by the Nessus solution on a monthly basis are responsible for producing millions of vulnerability data points. These outputs need to be prioritized and sorted so that the enterprise can make sense of the vulnerabilities and risks affecting its IT (information technology) landscape. The enterprise can then assign them to the appropriate personnel for review and mitigation. The Nessus Enterprise Web Tool (NEWT) was developed in 2014. NEWT uses a SQL (Structured Query Language) backend and SharePoint frontend to process vulnerability data to create reports for stakeholders. The following is a description of how NEWT automates the analysis of vulnerability data.

- **Import Data:** NEWT imports the files that are created from Nessus scanning. This process takes one to two (1-2) days. Data from SCCM and BigFix is also imported, along with Active Directory information, which is used as part of system owner identification.
- **Validate Data**: NEWT automatically flags Nessus events, which indicates scan failure. Much of the data from Big Fix and SCCM is normalized. The automated process takes three days, while manual analysis and report creation requires additional time.
- **Prioritize Vulnerabilities:** Vulnerabilities are currently prioritized using the Common Vulnerability Scoring System (CVSS) Base Score of the CVE to determine the severity ranking as Critical/High/Medium/Low, based on NIST guidance.[4]

While NEWT marks progress over the large spreadsheets that were used to distribute information on scan results in the past, the following challenges remain:

- Import and normalization of data can require a significant amount of time to include manual analysis. This increases the window of risk exposure and impacts the ability to achieve remediation compliance.
- NEWT may not scale well to support new requirements.
- Current prioritization does integrate VA data. The integration of VA data can provide business impact, and other technical factors related to projected risk, for automated prioritization analytics at the enterprise and then local level.

[4] https://nvd.nist.gov/vuln-metrics/cvss

2.3 Remediation

Once vulnerability data is prepared in NEWT, an action item is distributed to IT Operations (ITOPS) to commence the remediation phase. Due to the policy defined in the Veterans Affairs Intranet Quorum (VAIQ) #7294131, the required remediation timeframes are as follows:

TABLE 2: VA REMEDIATION TIMEFRAMES POLICY

Severity Rating	Remediation Requirement
Emergent	Tested and applied as soon as possible
Critical	30 Days
High	60 Days
Medium	90 Days
Low	Timeframe determined by the system owner

An action item is an internal email notification to provide context on a required action. The action item for remediation serves the following purposes:

- Notifies system owners to review vulnerability reports and commence remediation
- Requests review of IP address to system owner, mapping and correcting the data stored in NEWT
- Reviews remediation timeframes
- Guides system owners to record remediation progress in the Remediation Effort Entry Form (REEF), a form used to import data into the NEWT SQL database
- Requires review of the Authority to Operate (ATO) Mitigation Report in NEWT, a trending report related to vulnerability remediation that is used to track compliance with VA policy
- Acknowledges receipt and marks the start of the remediation phase

Once system owners access and acknowledge the NEWT reports, the remediation process begins. Although remediation progress is required to be recorded in NEWT, system owners must follow the VA change management process. This includes manually creating change orders, submitting them in the enterprise IT Service Management (ITSM) solution for change management, and recording changes on the implementation of changes. Patching devices, as part of remediation, use both automated and manual approaches. Table 3 outlines some of the primary tools currently deployed by VA for automated remediation of vulnerabilities.

TABLE 3: VA PATCHING AND REMEDIATION TOOLS

Patching Tool	Description
Microsoft System Center Configuration Manager (SCCM)	SCCM was acquired in 2007 for endpoint management and enterprise reporting at VA. In 2012, SCCM was upgraded so that it has some capacity to scan and update both Windows and Mac OS computers, with limitations.
IBM BigFix	IBM BigFix was acquired in 2008 to cover the gap in support of Mac endpoints. Since its acquisition, the use of IBM BigFix has evolved to manage a high percentage of VA Windows and Mac OS computers.
Heat LANrev	HEAT LANrev Client Management was procured by VA in 2012 to bring Mac iOS into compliance. VA uses this technology to patch a percentage of Mac iOS devices within the enterprise.

There are multiple challenges in the remediation phase that contribute to increased risk for VA.

- The remediation process designed through NEWT is disconnected from the change management process that is established for all enterprise hardware, software, and configuration changes. This can create duplicative efforts and increase the level of effort that is required to implement and track remediation.
- Patch management solutions do not have a well-defined scope to prevent solution overlap. This has led to conflicting data that must be analyzed and normalized.
- The remediation phase references the VA "Flaw Remediation SOP" (Standard Operating Procedure), which contains outdated information.
- The mapping of IP addresses to the system owner is being crowdsourced informally in NEWT; this means that system owners volunteer data from personal knowledge without an authoritative source. The creation of this informal data source can create problems during organizational changes because the informal data source is not linked to an authoritative one.

2.4 Mitigation

The mitigation phase is ongoing. Automated reporting is performed on a monthly basis. As a new monthly vulnerability scan is completed, NEWT automates the comparison of the most recent scan against the previous one. Then NEWT uses the delta to determine which items have been resolved. The items that are not resolved by the next scan are tracked using the NEWT REEF form. REEF information is used in part to create the monthly ATO mitigation reports. It is also manually uploaded to the FISMA team to display remediation statuses for other reporting. REEF automatically creates a ticket in the ITSM solution after the REEF entry is marked as completed.

While REEF is moving in the direction of closing gaps in the mitigation phase, there are still some challenges that remain:

- Without centralized governance over the VM process, root cause analysis has not been consistently successful in identifying and resolving systemic issues, preventing resolution of this material weakness.
- Remediation activities may be recorded in NEWT, the Governance, Risk Management, and Compliance (GRC) tool, or in the ITSM solution, or all three. Duplication of effort may occur. Conflicts could lead to questions on the integrity of the data.
- Responses have not been standardized on the mitigations for systems that are likely to fail automated remediation.

3 Future Capabilities

The future VM program will define a single strategy across the entire lifecycle to increase efficiency and meet compliance goals, while reducing risk. As seen in Figure 2, the VM program will improve risk management at VA by (1) performing root cause analysis to resolve challenges that impact VM efforts and shorten the lifecycle, and (2) applying a process of continuous improvement across all phases.

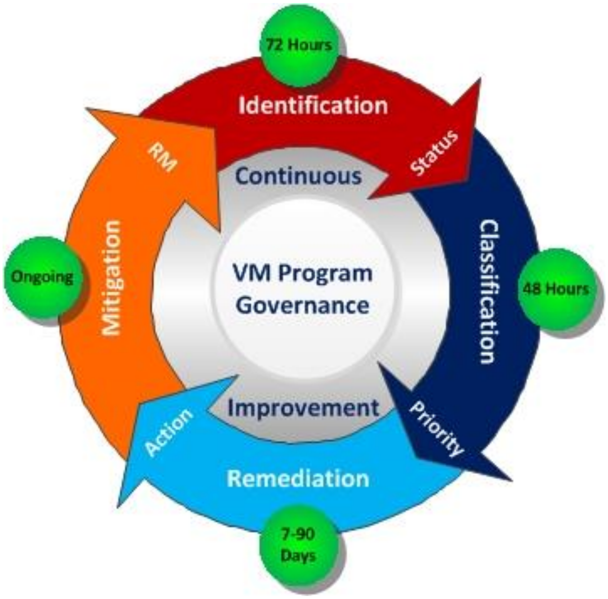


Figure 2: VM Lifecycle Overview

The VM program will align with NIST 800-40, Rev. 3, and VA Handbook 6500. The following table maps future capabilities to business benefits. It provides more detail on how the future capabilities will deliver identified business benefits to achieve the desired results.

TABLE 4: MAPPING OF FUTURE CAPABILITIES TO BUSINESS BENEFITS

Business Benefits	Future Capability Description
VM Program Governance	VM governance will provide tactical direction to achieve program objectives. This will include establishing authority, policy, and procedures to meet compliance and strategic goals.
Unified Strategy for Enterprise Vulnerability Management	A single strategy will align tools to specific objectives to create authoritative data in an efficient manner. Processes will be integrated and leverage automation to reduce the lifecycle timeframe.
Federal and VA Compliance	The VM program will coordinate with the CDM program to increase security through automated testing and reduce risk by minimizing the window between vulnerability identification and remediation or mitigation.
Increased Security/Decreased Risk Exposure	VM solutions will support near real-time reporting that will increase visibility and provide actionable data for managing risk.

3.1 VM Program Governance

A permanent enterprise patch and vulnerability program was established by Infrastructure Operations (IO) Security Management, under the direction of ITOPS, as of June 2017. The owner of the VM program will define governance through the following actions:

- Initiate a formal committee to collaborate with all stakeholders in the VM process, with sufficient authority to implement strategy and resolve systemic issues directly or indirectly.
- Integrate with other areas, such as Configuration Management, Change Management, Network Security, and Risk Management, to identify roadblocks and implement recommended improvements.
- Identify appropriate roles and responsibilities to support VM strategy and coordinate updates of policy, as needed.
- Define VM processes that support both on premise and cloud-based applications.

- Define key performance indicators and other metrics to measure compliance, program success, and alerts for indicators that signal the need for further action.

3.2 Identification

The identification phase will discover all assets on the network and provide authoritative data on the known vulnerability status for each endpoint. This phase will continue to be able to assess compliance against required controls, including FISMA, USGCB, and DISA STIGs. The Department of Homeland Security (DHS) CDM goal of seventy-two (72) hours for data currency places a heavy emphasis on automated and repeatable processes.

The identification phase will include the following actions to provide required capabilities:

- Leverage CDM solutions to perform both active and passive device discovery to ensure comprehensive device identification.
- Leverage CDM solutions first, and others as necessary, to assess current vulnerabilities.
- Define a single solution for vulnerability assessment to include virtual, cloud, mobile, and Special Purpose Systems (SPS), as possible. This will be supplemented by other solutions only where the single solution cannot assess a specific device or application type. The VM program will prevent solution overlap in design, with the goal of providing comprehensive coverage, while maintaining an authoritative vulnerability data source for each host.
- Implement agentless and agent-based assessment, as appropriate, to manage the impact of vulnerability identification on the network, reduce dependency on service accounts, and increase coverage for devices that are not attached to the VA network at all times.
- Establish appropriate permissions to ensure accurate vulnerability assessments.
- Automate the retesting of devices where the assessment failed.
- Meet the DHS CDM goal of 72 hours for data currency.
- Ensure all solutions hosting authoritative vulnerability data can integrate with the solution performing vulnerability classification and analysis.

3.3 Classification

It is critical that the classification phase apply automation to create actionable data in a timely manner. The data generated by the identification phase will be fused with available VA data sources to apply adjusted risk scoring that can be used for prioritization. Prioritization will consider the exposure of the affected system as well as the potential business impact of exploitation. The resulting information needs to be provided to system owners within the classification solution. The information should not be presented in manual reports, as the status of systems will be dynamically updated. This will allow system owners to see progress and new vulnerabilities in a more continuous process. The VM program will identify a solution for classification which:

- Supports automated ingestion, or query of vulnerability data, that is generated during the identification phase; it also supports asset management, software inventory, and other solutions of varying formats that are required to perform analysis for prioritization
- Provides the ability to automate the quality control of raw data:
    - Identifies false positives, by validating scan results that indicate a missing software patch against the authoritative software inventory for the endpoint, when available
    - Identifies failed scans
- Provides automated alerting, data analysis, and historical reporting for trending
- Supports dashboards or dynamically updated reports that can be assigned to users
- Supports varying formats and the manual entry of vulnerabilities that are identified outside of the primary identification process

The VM program will review the Enterprise Audit Design Pattern for areas applicable to the VM program for best practice recommendations for the integration of vulnerability and threat intelligence data, which may be used as a factor in prioritization.

3.4 Remediation

The remediation phase will provide vulnerability analysis results in a timely manner and coordinate with change management, configuration management, and other areas to create integration that reduces the window of risk exposure. In this area, the VM program will:

- Identify a standard workflow for remediation that is performed as part of the VM lifecycle.
- Use an authoritative data source for identification of system owners to asset mapping for assignment of vulnerability remediation. Coordinate with the VA Chief Information Officer (CIO) if an authoritative data source is not defined.
- Clearly define the definition for the start time and end time for remediation timeframes to create consistent application of policy across all stakeholders.
- Integrate the solution used for classification with ITSM tools to create efficiencies.
- Confer with the Data Governance Council if creating new authoritative data sources. When reporting is required on the progress of change orders that are related to remediation, it is recommended to link to information that is captured in enterprise

ITSM tools, without recreating the data elsewhere. Linking to information captured in the Plan of Action and Milestones (POA&M) is recommended for the same purpose.

3.5 Mitigation

The remediation phase retains some inherent risks. While the time to remediate some vulnerabilities will create a window of risk, others may not be able to be remediated at all, due to a lack of vendor support or impact to operations. The goal of the mitigation phase is to lower risk to acceptable levels until longer term solutions can be developed. This makes RCA a critical capability that will be performed by the VM program during this phase. When the remediation phase is insufficient to control risk, the VM program will incorporate the following actions:

- Coordinate with the Office of Quality, Privacy, and Risk (QPR) to identify processes for how VM will support enterprise risk management activities.
- Collaborate with other internal organizations to identify and resolve dependencies that degrade VM program performance.
- Integrate with internal network security organizations to identify network security countermeasures, such as virtual patching and traffic filtering to lower risk.
- Identify standard responses that can be reused for systems that create increased risk, including SPS, medical devices, systems that cannot be remediated, and systems with change management processes that fail to meet remediation deadlines. One example would be to move applications that cannot support secure authentication methods into a logical zone with a proxy that can support compliant authentication.
- Identify systems that should be monitored as high risk when they are consistently unable to meet remediation deadlines, based on their standard change management process. This will trigger a root cause analysis to determine the cause and long term mitigating actions.
- Contribute to the refinement of security controls and standards used for the software development lifecycle (SDLC) by providing vulnerability metrics and feedback on custom software that is released into VA production.
- Analyze the creation of a Bounty Program[5] as an option to enhance the security of VA's internet-facing applications and services. This type of program would reward participants that identify weaknesses in internet-facing VA applications and disclose the details to VA so that the issue can be corrected. Contact the Department of Defense (DoD) for lessons learned on their program and the General Services Administration (GSA) for potential collaboration.

[5] https://www.defense.gov/News/News-Releases/News-Release-View/Article/1009956/dod-announces-digital-vulnerability-disclosure-policy-and-hack-the-army-kick-off/

3.6 Alignment to the One-VA Technical Reference Model (TRM)

The EDP and the One-VA TRM are authoritative sources that can be combined to lead to a more coordinated approach to project management and compliance. It identifies the technologies and standards within the VA production computing environment that can be used at VA; and it determines the conditions for how they can be used. The One-VA TRM also enables users to request an assessment of a new technology, or a new version of an existing technology, and to interpret assessment results. The List of Approved Tools and Standards Table below enables users to easily search for comparable technologies at the One-VA TRM.

TABLE 5: LIST OF APPROVED TOOLS AND STANDARDS FOR VULNERABILITY MANAGEMENT

TRM Domain	TRM Area	TRM Category	Example Technologies	Example Standards
Security	Data Security	Data Loss Prevention	Microsoft BaseLine Security Analyzer	N/A
	Network Security	Security Administration		
	Data Security	Data Loss Prevention	AppDetectivePro	N/A
	Network Security	Network Auditing		
	Network Security	Network Access Control *and* Network Auditing	HyTrust CloudControl	N/A
		Network Auditing	Tenable Nessus, NMAP, Security Content Automation Protocol (SCAP) Compliance Checker, Core Impact, SNScan	Extensible Configuration Checklist Description Format (XCCDF), Open Vulnerability Assessment Language (OVAL), Security Content Automation Protocol (SCAP)
			Burp Suite	N/A
		Network Intrusion and Prevention	Rapid7 AppSpider	N/A
	Platform Security	Application Security	HP Fortify Webinspect	N/A
			IBM Security AppScan	N/A

TRM Domain	TRM Area	TRM Category	Example Technologies	Example Standards
Systems Management	Systems Management Tools	Application Management	IBM BigFix	N/A
		Remote Desktop Management	Heat LANrev	N/A
		System Change and Configuration *and* Data Center Automation Software	Microsoft System Center Configuration Manager (SCCM)	N/A
			Shavlik Patch	N/A
		System Change and Configuration	Red Hat	N/A

3.7 Alignment to VIP

The Veteran-Focused Integration Process (VIP) is a Lean-Agile Framework that serves the interest of Veterans through efficiently streamlining activities that occur within the enterprise. VIP unifies IT delivery oversight and delivers IT products more securely and predictably. VIP is the follow-on framework from the Project Management Accountability System (PMAS) for the development and management of IT projects. VIP propels VA with even more rigor toward the Veteran-focused delivery of IT capabilities.

More information can be found at https://vaww.oit.va.gov/veteran-focused-integration-process-vip-guide/.

4 Use Cases

4.1 Web Application Vulnerability

4.1.1 Purpose

A vulnerability is reported on a common web application framework. The vulnerability can result in compromise to the underlying system. The vulnerability poses a significant risk to Veteran data. Prioritization is needed to remediate the highest risk systems first, as not all vulnerable systems can be remediated at once.

4.1.2 Assumptions

- The web application framework is in use at VA.
- Relevant system information is available to the solution used in the classification phase.
- The web application framework is used for internal and internet-facing applications.

4.1.3 Use Case Description

1. A new vulnerability is reported in a common web application framework used for hosting VA websites. The flaw could lead to compromise of the underlying operating system and expose sensitive data.
2. The updated signature is imported into the vulnerability identification solution. The longest possible delay is 72 hours for confirmation of vulnerable systems and is based on the audit cycle.
3. VM analysts project vulnerable systems in advance by querying authoritative software inventory solutions for the specified versions of software.
4. The vulnerability discovery phase is completed and vulnerable hosts have been identified. Prioritization of remediation is automatically calculated using system information such as FISMA rating, hosting of sensitive information, internet accessibility, and average timeframe for remediation.
5. Prioritization is reviewed against available network security countermeasures and updated as necessary.
6. System owners are notified to review their dynamically updated dashboard for a prioritized action item list.

4.2 Monthly Patch Management Remediation

4.2.1 Assumptions

VA receives certain vendor security patches on a monthly basis. VA desires to streamline the process as much as possible to perform the remediation.

4.2.2 Use Case Description

- The patches are released by the vendor on a regular basis.
- Information on CVEs and CVSS scores that are related to the patches are available.
- The systems to which the patches will be applied are already known.

4.2.3 Use Case Description

1. The VM program is streamlining the process for applying monthly security patches released by a vendor.
2. The systems are readily identified in the VM classification solution. When vulnerability identification is completed, the vulnerabilities for the vendor software are identified.
3. The VM classification solution is integrated with the ITSM change management solution to allow data export for the efficient creation of change orders.

4. The vulnerability discovery solution updates every 72 hours and dynamically updates reports where system owners can track remediation progress.
5. Integration with the ITSM solution allows automated identification of systems with closed change orders, where remediation has not been verified as completed by a vulnerability audit of a later date.
6. Reports are easily created for closure of POA&Ms, where applicable.

4.3 Vulnerability Management Reporting Challenges

4.3.1 Purpose

The VM process requires visibility into the risk profile of devices and the ability to effectively plan and perform remediation as part of risk management. The purpose of this use case is to review how reporting and analytics of vulnerability data supports these goals.

4.3.2 Assumptions

- The reporting requirements for VM are defined and met through a reporting solution.
- The reporting solution may be part of an existing enterprise shared service.

4.3.3 Use Case Descriptions

1. VA is updating its scanning strategy in compliance with the DHS CDM requirements for 72-hour data currency. As stakeholders still need to perform trending using historical data, this will cause a data volume increase of at least 10x the current levels.
2. The VM governance team has already planned for a reporting solution that can scale quickly to support changes to the VA enterprise, and adopted an enterprise shared service (ESS) for this requirement. The ESS includes support for real-time dashboards, as well as efficient historical searches across large sets of data.
3. The VM governance group coordinates with ITOPS to confirm the expected scaling of ESS to meet operational needs. Changes to the data set require dashboards to be updated and reports to continue to provide proper alerts, automated prioritization analysis, and trending. The VM governance group is able to obtain surge support to complete this task quickly to prevent compliance gaps, as the ESS is built using commercial off-the-shelf (COTS) products that are used by other stakeholders across VA.

APPENDIX A. SCOPE

This EDP focuses on the process for identifying, classifying, remediating, and mitigating vulnerabilities found within VA's IT infrastructure that is integral to both computer and network security. A robust VM program should be implemented within the enterprise in order to effectively remedy vulnerabilities identified in operating system (OS) databases, applications, and other network devices. This EDP makes recommendations for implementing standardized enterprise-wide VM practices that are based on industry best practices.

Topics that are out of scope for this EDP, but may be referenced, include the following:

- Configuration management and baselines
- Removing unauthorized software by removing user permissions and scanning
- Patch management
- Cloud computing

Document Development and Maintenance

This EDP was developed collaboratively with internal stakeholders from across the Department, including participation from VA's OIT, the EPMO, the Office of Information Security (OIS), ASD, and Information Technology Operations and Services (ITOPS). In addition, the development effort included engagements with industry experts to review, provide input, and comment on the proposed pattern. This document contains a revision history and revision approval logs to track all changes. Significant updates will be coordinated with the Government lead for this document, who will also facilitate stakeholder coordination and subsequent re-approval.

Appendix B. Definitions

This appendix provides definitions for terms used in this document.

Key Term	Definition
Authority to Operate (ATO)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, based on the implementation of an agreed-upon set of security controls
BigFix	A systems-management software product developed by IBM for managing large groups of computers running Windows, Mac OS X, VMware ESX, Linux or UNIX, as well as various mobile operating systems such as Windows Phone, Symbian, iOS, and Android
Continuous Diagnostics and Mitigation (CDM)	A program that is a dynamic approach to fortifying the cybersecurity of government networks and systems; CDM provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first
Common Vulnerabilities and Exposures (CVE)	A system that provides a reference-method for publicly known information security vulnerabilities and exposures
Common Weakness Enumeration (CWE)	A software community project that aims to create a catalog of software weaknesses and vulnerabilities; the goal of the project is to better understand flaws in software and to create automated tools that can be used to identify, fix, and prevent those flaws
Configuration Management (CM)	The process of identifying, controlling, verifying, and showing the relationship among all infrastructure components
Configuration Management Database (CMDB)	The repository that stores the identity of each component of the information infrastructure, to include hardware, software, and documentation assets; documentation is included in the database that is procedural, referential and instructional
Continuous Monitoring	Maintains ongoing awareness to support organizational risk decisions (See *Information Security Continuous Monitoring)*

Key Term	Definition
Continuous Readiness Information Security Program (CRISP)	A VA program that transformed how VA information is accessed, protected, and transferred within and outside the Department; CRISP offers a three-pronged approach to improve information security
Common Vulnerability Scoring System (CVSS)	A free and open industry standard for assessing the severity of computer system security vulnerabilities; CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber-attacks
Database	A data asset that is comprised of data records
Defense Information Systems Agency (DISA)	A United States Department of Defense (DoD) combat support agency composed of military, federal civilians, and contractors; DISA provides information technology (IT) and communications support to the President, Vice President, Secretary of Defense, the military services, the combatant commands, and any individual or system contributing to the defense of the United States
Enterprise Design Pattern (EDP)	Capability guidance documents that identify repeatable, best practice approaches to addressing recurring technical challenges impacting VA's ability to improve and evolve information security, advance agile interoperability and information sharing, and reduce the total lifecycle cost of IT
Enterprise Shared Services (ESS)	A service-oriented architecture service that is visible and can be accessed by users across the enterprise, subject to appropriate security and privacy restrictions
Federal Information Security Management Act (FISMA)	United States legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002
Governance, Risk Management, and Compliance (GRC)	A discipline that aims to synchronize information and activity across governance, risk management, and compliance in order to more efficiently share, more effectively report activities, and avoid wasteful overlaps
General Services Administration (GSA)	An independent agency of the United States government to help manage and support the basic functioning of federal agencies

Key Term	Definition
Heat LANrev (formerly Absolute Manage)	Software used by VA to manage Mac iOS systems; this software has the capability to manage all VA endpoints from a single console, including PC, Mac, iOS, Android, and Windows phone devices; HEAT LANrev can also be deployed as a complete asset management solution, as well as a stand-alone MDM solution
IBM BigFix	A systems-management software product developed by IBM for managing large groups of computers running Windows, Mac OS X, VMware ESX, Linux or UNIX, as well as various mobile OSs such as Windows Phone, Symbian, iOS, and Android
Information Security Continuous Monitoring (ISCM)	Ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions
Information Technology Operations and Services (ITOPS)	The set of all processes and services that are both provisioned by an IT staff to their internal or external clients and used by themselves, to run themselves as a business; the term refers to the application of operations management to a business's technology needs
Information Technology Service Management (ITSM)	An entirety of activities directed by policies, organized and structured in processes and supporting procedures that are performed by an organization to plan, design, deliver, operate, IT services offered to customers
Internet Protocol (IP)	The principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries; its routing function enables internetworking and essentially establishes the Internet
Malicious Software	The umbrella term is used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs; it can take the form of executable code, scripts, active content, and other software.
Mobile Device Management (MDM)	Software that secures, monitors, manages, and supports mobile devices deployed across mobile operators, service providers, and enterprises; MDM functionality includes over-the-air distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones and smartphones and tablet devices
Nessus	The Tenable Nessus Scanner is a COTS vulnerability and compliance assessment solution

Key Term	Definition
Nessus Enterprise Web Tool (NEWT)	A custom VA solution for managing vulnerability data based on Microsoft SQL and SharePoint
National Institute of Standards and Technology (NIST)	A measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce; its mission is to promote innovation and industrial competitiveness
Office of Inspector General (OIG)	A generic term for the oversight division of a federal or state agency aimed at preventing inefficient or illegal operations within their parent agency; such offices are attached to many federal executive departments, independent federal agencies, as well as state and local governments
Office of Information Security (OIS)	The OIS is the primary state government authority charged with ensuring the confidentiality, integrity, and availability of state systems and applications, and ensuring the protection of state information assets.
Office of Information and Technology (OIT)	Provides adaptable, secure, and cost-effective technology services across VA, managing VA's IT assets and resources, and delivering technology and expertise that supports Veterans and their families
Office of Personnel Management (OPM)	An independent agency of the United States government that manages the civil service of the federal government
Office of Quality, Privacy, and Risk (QPR)	QPR leads OIT's performance management, process improvement, and oversight efforts in the areas of quality, risk management, organization development, and compliance
Operating System (OS)	A system software that manages computer hardware and software resources and provides common services for computer programs
Software Patch	A software update that fixes or improves a computer application or its supporting data
Patch Management	The process for identifying, acquiring, installing, and verifying patches for products and systems
Personally Identifiable Information (PII)	PII is information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Key Term	Definition
Plan of Action & Milestones (POA&M)	A method used to identify and track tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones to be passed in accomplishing the task, and scheduled dates for reaching each milestone
Protected Health Information (PHI)	Any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a business associate of a Covered Entity), and can be linked to a specific individual
Remediate	The act of correcting vulnerability or eliminating a threat; three possible types of remediation include installing a patch, adjusting configuration settings, or uninstalling a software application
Remediation Effort Entry Form (REEF)	A form used to import data into the SQL database of VA’s custom solution “NEWT”
Risk Management (RM)	The identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events[1] or to maximize the realization of opportunities
DISA Security Technical Implementation Guides (STIG)	A cybersecurity methodology for standardizing minimum-security protocols within networks, servers, computers, and logical designs to enhance overall security, as designed by DISA
Sensitive Personal Information (SPI)	This sensitive information can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context
System development lifecycle process (SDLC)	A systems development life cycle is composed of a number of clearly defined and distinct work phases which are used by systems engineers and systems developers to plan for, design, build, test, and deliver information systems
Splun	A COTS product used to collect, index and analyze structured and unstructured data generated by devices
Structured Query Language (SQL)	A domain-specific language used in programming and designed for managing data held in a relational database management system (RDBMS), or for stream processing in a RDSMS
Strategic Technology Alignment Team (STAT)	A VA group that leverages the VIP framework to ensure alignment with Design, Engineering and Architecture (DE&A) requirements and compliance with related VA policy for new projects

Key Term	Definition
Systems Center Configuration Manager (SCCM)	A systems management software product developed by Microsoft for managing large groups of computers running Windows NT, Windows Embedded, macOS (OS X), Linux or UNIX, as well as Windows Phone, Symbian, iOS, and Android mobile Oss; Configuration Manager provides remote control, patch management, software distribution, OS deployment, network access protection and hardware and software inventory
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service
Threat Analysis	A threat analysis is an examination of threat sources against system vulnerabilities to determine the threats for a system in a particular operational environment
Technical Reference Model (TRM)	A component-based technical framework used to categorize the standards and technologies that support and enable the delivery of service at VA
United States Government Configuration Baseline (USGCB)	Initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies; the USGCB baseline evolved from the Federal Desktop Core Configuration mandate; the USGCB is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain effective configuration settings focusing primarily on security
User Behavior Analytics (UBA)	A cybersecurity process about detection of insider threats, targeted attacks, and financial fraud; UBA tools use a specialized type of security analytics that focuses on the behavior of systems and the people using them
Veteran-Focused Integration Process (VIP)	A Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. VIP is a significant step forward for VA, allowing greatly-needed IT services to be delivered to Veterans more frequently
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

Key Term	Definition
Vulnerability Management (VM)	A security practice specifically designed to proactively mitigate or prevent the exploitation of IT vulnerabilities which exist in a system or organization; the process involves the identification, classification, remedy, and mitigation of various vulnerabilities within a system

APPENDIX C. ACRONYMS AND ABBREVIATIONS

The following table provides a list of acronyms and abbreviations that are applicable to and used within this document.

Acronym	Description
A&A	Assessment and Authorization
ATO	Authority to Operate
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CM	Configuration Manager
CMDB	Configuration Management Database
COTS	Commercial off-the-shelf Software
CRISP	Continuous Readiness Information Security Program
CVSS	Common Vulnerability Scoring System
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DE&A	Design, Engineering and Architecture
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
EDP	Enterprise Design Pattern
ESS	Enterprise Shared Service
FISMA	Federal Information Security Management Act
GRC	Governance, Risk, and Compliance
GSA	General Services Administration
IO	Infrastructure Operations
IP	Internet Protocol
IT	Information Technology
ISCM	Information Security Continuous Monitoring
ITOPS	Information Technology Operations and Services
ITSM	Information Technology Service Management
MDM	Mobile Device Management
NEWT	NESSUS Enterprise Web Tool
NIST	National Institute of Standards and Technology
OS	Operating System
OIG	Office of Inspector General

Acronym	Description
OIS	Office of Information Security
OIT	Office of Information and Technology
OPM	Office of Personnel Management
PHI	Protected Health Information
PII	Personally Identifiable Information
PMAS	Project Management Accountability System
POA&M	Plan of Action and Milestones
QPR	Office of Quality, Privacy, and Risk
RDBMS	Relational Database Management System
RDSMS	Relational Data Stream Management System
REEF	Remediation Effort Entry Form
RCA	Root Cause Analysis
RM	Risk Management
SCCM	System Center Configuration Manager
SDLC	Software Development Lifecycle Process
SOP	Standard Operating Procedure
SPS	Special Purpose Systems
SPI	Sensitive Personal information
SQL	Structured Query Language
STAT	Strategic Technology Alignment Team
STIGs	Security Technical Implementation Guides
TRM	Technical Reference Model
UBA	User Behavior Analytics
USGCB	United States Government Configuration Baseline
VA	Department of Veterans Affairs
VA ETA	VA Enterprise Technical Architecture
VAIQ	Veterans Affairs Intranet Quorum
VIP	Veteran-Focused Integration Process
VM	Vulnerability Management

APPENDIX D. REFERENCES, STANDARDS, AND POLICIES

This EDP is aligned to the VA Enterprise Technical Architecture (ETA) and the following VA OIT references and standards that are applicable to all new applications developed at VA.:

#	Issuing Agency	Applicable Reference/ Standard	Purpose
1	VA	VA Directive 6551	Establishes a mandatory policy for establishing and utilizing Enterprise Design Patterns by all Department of Veterans Affairs (VA) projects developing information technology (IT) systems in accordance with VA's Office of Information and Technology (OIT) integrated development and release management process, the Veteran-focused Integration Process (VIP).
2	VA	VA Directive 6004	Establishes Department of Veterans Affairs (VA) policy and responsibilities regarding Configuration, Change, and Release Management Programs for implementation across VA. This directive applies to all VA related components and information technology resources, including contracted Information Technology (IT) systems and services.
3	VA OIS	VA Handbook 6500	Directive from the OIT Office of Information Security (OIS) for establishment of an information security program in VA, which applies to all applications that leverage Enterprise Shared Services (ESS).
4	VA OIS	VA Handbook 6500.3	This handbook provides the next level of policy to establish requirements and responsibilities for Assessment and Authorization (A&A) and to establish VA's Information Security Continuous Monitoring (ISCM) program. Additional procedures for A&A and the ISCM program will be distributed by the Office of Information and Technology.

#	Issuing Agency	Applicable Reference/ Standard	Purpose
5	NIST	800-40-3	NIST 800-43, Rev. 3 is designed to assist organizations in understanding the basics of enterprise patch management technologies. It explains the importance of patch management and examines the challenges inherent in performing patch management. It also provides an overview of enterprise patch management technologies and briefly discusses metrics for measuring the technologies' effectiveness and for comparing the relative importance of patches.
6	NIST	800-63-2	This recommendation provides technical guidelines to agencies for the implementation of electronic authentication (e-authentication).
7	VA OIS	FY2016-2018 Enterprise Roadmap	This document outlines OITs transformation for delivering a rapid succession of improvements based on the institutionalization of a new set of capabilities to drive improved outcomes; the elimination and mitigation of material weaknesses; and the stabilization and streamlining of core process and platforms.
8	NIST	820-137	This publication specifically addresses the assessment and analysis of security control effectiveness and of organizational security status in accordance with organizational risk tolerance.
9	NIST	800-39	This publication provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems.

#	Issuing Agency	Applicable Reference/ Standard	Purpose
9	Gartner	A Comparison of Vulnerability and Security Configuration Assessment Solutions.	This assessment adopted a narrow definition of vulnerability assessment and provided a comparison of the solution based on that definition.
10	VAIQ	7294131	This memo issues remediation requirements for each vulnerability categorization.

Disclaimer: This document serves both internal and external customers. Links displayed throughout this document may not be viewable to all users outside the VA domain. This document may also include 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.