Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

Web Applications Security Cross-Cutting Project – A Federal Government Assessment of Publicly Facing Web Applications

CIGIE IT Committee

Washington, DC October 3, 2017

This page is intentionally left blank

Executive Summary

Purpose

This project assessed how well Federal agencies and other designated Federal entities are able to identify, assess, and resolve security vulnerabilities on their publicly accessible web applications through a Council of the Inspectors General on Integrity and Efficiency (CIGIE) cross-cutting project.

What We Did

Led by the U.S. Department of Housing and Urban Development (HUD) Office of Inspector General (OIG), nine participating OIGs conducted an assessment of their agency's publicly accessible web applications using a standard testing approach developed by the CIGIE web application cross-cutting project group. The OIG testing consisted of identifying web applications, scanning those applications for security weaknesses, conducting an in-depth review of selected systems, and reviewing their agency's web application related security policies and procedures. An additional 22 OIGs responded to a survey for information about their agency's web application security practices.

What We Recommend

In addition to the recommendations provided in each section of this report, we suggest Federal agencies conduct a review of all their agency's web applications to ensure they have been properly inventoried, authorized, and secured using web application best business practices such as Open Web Application Security Project and National Institute of Standards and Technology guidance. Furthermore, we recommend that Office of Management and Budget require agencies to include web applications in current security processes and policies or develop agency processes and policies to properly secure their web applications.

What We Found

The Federal Government relies extensively on Web based information technology systems, some of which are managed, hosted, provided and used by third parties to assist in Government operations. Federal web applications are at increased risk of unauthorized access due to unresolved security vulnerabilities and a lack of proper application implementation. Unauthorized access can lead to many problems for Federal agencies, such as a breach of sensitive data, the unavailability of the application for authorized use, and providing the basis for launching additional attacks. As part of this consolidated web application review, nine participating Offices of Inspector General (OIG) (see Appendix B) collected data from multiple tests and methods as outlined in the "Objective, Methodology, and Scope" section of this report.[1] An additional 22 OIGs participated in a web application survey to gather additional data from across the Federal Government. Once the OIGs validated their results, they transmitted the results to the HUD OIG for consolidation. Due to variances in agency networks and available OIG resources, not all nine OIGs tested every element of the methodology.

The majority of the participating OIGs have issued reports or plan to issue reports to their agency with agency specific recommendations.

The testing that the OIGs conducted as part of the CIGIE initiative indicated the following three significant deficiencies across the agencies reviewed.

Incomplete and Inaccurate Inventory: OIGs found that 75 percent of the agencies reviewed did not have a complete and accurate inventory of web applications. An inventory is essential for understanding the web applications that need to be protected. It is a requirement for ensuring appropriate security is in place.

Many Critical and High Severity Vulnerabilities Found: OIGs identified thousands of security vulnerabilities across the participating agencies. Almost 50 percent of those vulnerabilities fell into the high and critical severity rating, indicating they pose substantial risk to the web application and should be prioritized for resolution.

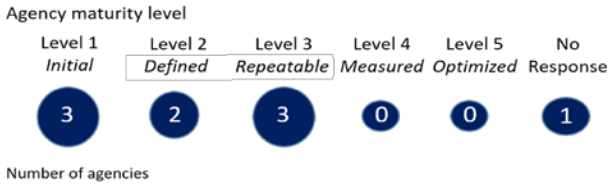
Inconsistent and Poorly Implemented Web Security Policies and Processes: OIGs determined that their agencies were generally not consistently implementing web security policies and processes. The review also revealed that agencies generally did not consistently apply web application policies and processes. Having well-defined, repeatable, and consistently implemented processes is critical to reducing the possibility of an attacker successfully exploiting a single weakness.

Not having a complete inventory of applications, an inability to properly secure those applications, and a lack of process and consistent policy implementation reduced the security posture of many web applications reviewed in this assessment. We used the Federal Information Security Modernization Act Inspector General maturity model of five levels to assess the effectiveness of

[1] Due to the technical requirements, not all participating OIGs reviewed all phases in the methodology.

reviewed agency web application security programs with the lowest level (level 1) being “Initial” and the highest level (level 5) being “Optimized.” No agencies reviewed reached a level 4 or 5 maturity for overall web application process and procedure implementation. Three agencies achieved only level 1, 2 agencies achieved level 2, and 3 agencies achieved a level 3 maturity level. One OIG did not assess their agency using the model (see figure below).

Assessment of Agency Maturity Model for Establishing a Web Application Policy and Procedure Security Program



Many of the participating OIGs found vulnerabilities that could easily be compromised and exploited if the vulnerabilities were not remediated. In one instance, an OIG discovered that its agency’s network had become compromised due to vulnerabilities in their web application environment. Until these issues are addressed, these Federal agencies will continue to face increased risk of unauthorized access to their publicly accessible web applications and the data that these applications access.

Table of Contents

List of Tables and Figures

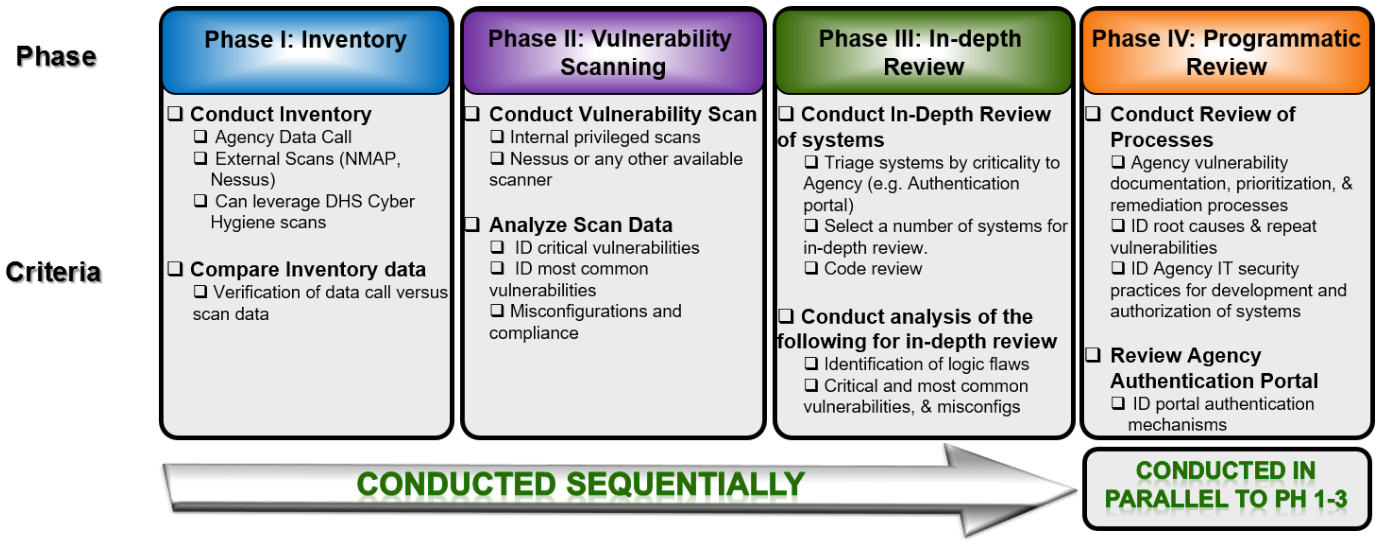
ONE

OBJECTIVE, METHODOLOGY, AND SCOPE

The U.S. Department of Housing and Urban Development (HUD) Office of Inspector General (OIG) led this review, which includes input coming from reviews conducted by each participating OIG. The reviews were conducted from February 2016 through February 2017. The objective of this project was to assess and determine the extent and efficiency of agencies' efforts to identify and assess vulnerabilities on publicly accessible web applications[2] and mitigate the most severe vulnerabilities. In addition, where appropriate, OIGs assessed efforts of agencies to control or reduce the number of those publicly accessible web applications. Nine OIGs used the following phased approach (see Figure 1) and a standardized testing methodology to conduct reviews of their agencies and collect data.[3]

- **Phase 1 (inventory review)** focused on obtaining a complete inventory of web applications. OIGs validated their agencies' inventories with automated tests such as external network scans and manual review of internet registration data.
- **Phase 2 (vulnerability assessment)** used automated tools to scan hardware and software that supported applications identified during Phase 1. The scanning tools attempted to detect security configuration errors and known software vulnerabilities.
- **Phase 3 (in-depth application review)** consisted of in-depth automated and manual testing on a sample of applications from the inventory identified in Phase 1. OIGs typically limited the scope of this phase to three high risk web applications.
- **Phase 4 (policy and procedure review)** assessed the effectiveness of the agency's web application security program through a review of policies, procedures, and staff interviews.

Figure 1. Assessment phases



[2] As defined by OMB Memorandum M-15-13, publicly accessible websites, applications, and services are defined as online resources and services available over HTTP or HTTPS over the public internet that are maintained in whole or in part by the Federal Government and operated by an agency, contractor, or other organization on behalf of the agency. They present government information or provide services to the public or a specific user group and support the performance of an agency's mission. This definition includes all web interactions, whether a visitor is logged-in or anonymous.

[3] Due to resource limitations in the nine participating OIGs, four of the nine OIGs conducted Phase 3, and eight of the nine OIGs conducted Phase 4. All nine OIGs conducted Phases 1 and 2.

This project used the Federal Information Security Modernization Act (FISMA), National Institute of Standards and Technology (NIST)[4] special publications, and publications from the Open Web Application Security Project (OWASP)[5] to establish Federal Government best practices and to identify critical risks faced by web applications. These publications included NIST SP 800-53 revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-44 revision 2, *Guidelines on Securing Public Web Servers*, SP 800-95, *Guide to Secure Web Services*, and SP 800-115, *Technical Guide to Information Security Testing and Assessment.* The project also used the OWASP Testing Guide to identify effective procedures for assessing vulnerabilities, including the OWASP Top 10 risks. Finally, we used the Center for Internet Security (CIS)[6] critical security controls as a source of effective actions that could be taken to address risks.

The scope of this project included all publicly available web applications operated by the participating agencies. Not all agencies completed all phases due to resource constraints, such as staffing and budget. The most common difference between the OIG reviews was to omit Phase 3.[7] Due to the population size, these results cannot be projected government-wide. These results, however, provide evidence of common themes and trends related to public government websites. OIGs and their agencies should consider incorporating web application reviews, if not already done, in their information technology (IT) risk management processes. This project group received data from two sources.

- Project participant data. Nine[8] OIGs participated in the project and provided data on their agencies based on the criteria for the phases above.
- Additional OIG Survey. Twenty-two OIGs responded to a 13 question web application survey that provided additional supporting data to the participating project OIGs.

We encourage the OIG community to use this as a general framework to focus on specific areas to build IT audit, evaluation, and assessment programs.

[4] To promote United States innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security. Source: https://www.nist.gov/about-nist/our-organization/mission-vision-values

[5] OWASP is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Source: https://www.owasp.org

[6] CIS is a nonprofit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. Source: https://www.cisecurity.org/about-us/

[7] Four of the nine OIGs conducted Phase 3 in their reviews of their agencies.

[8] OIGs that contributed to this report are listed by agency size or type in Appendix B.

TWO

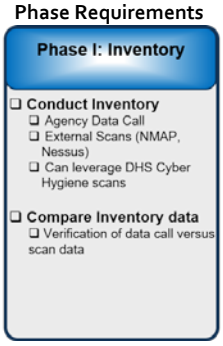
RESULTS OF REVIEW

IMPROVEMENTS ARE NEEDED FOR WEB APPLICATION INVENTORY (PHASE ONE)

Requirement:

The first phase of the project determined the participating agencies' capabilities for maintaining an accurate and complete inventory of publicly accessible web applications and inventory responsibilities. To do this, the participating OIGs conducted an inventory using several methods such as scanning for web applications and data calls and then comparing all the inventory data (see Figure 2). The areas reviewed in this phase dealt with the maintenance of an accurate and complete inventory of public facing web applications and inventory responsibility. OIGs used manual and automated scanning methods in this phase to determine the number of web applications at each agency. The OIGs also collected data through surveying agency sub-components.

Figure 2. Inventory Assessment Phase Requirements

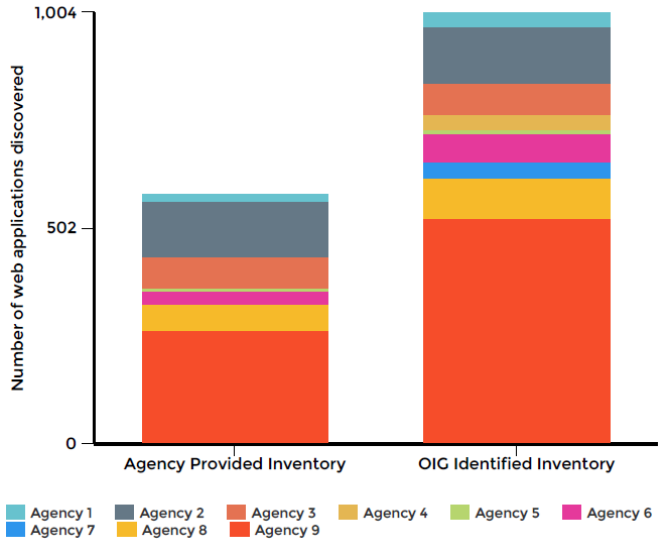


The Office of Management and Budget (OMB) requires Federal agencies to follow NIST guidance. According to NIST, Federal agencies need to develop and document an inventory of information system components that: (1) accurately reflects the current information system, (2) includes all components within the authorization boundary of the information system, and (3) includes the granularity deemed necessary for tracking and reporting. Per NIST and FISMA, effective inventories should also identify the application or system owner and system interface. Furthermore, agencies should verify that all components within the authorization boundary of the information system are not duplicated in other information system component inventories.

Results:

Analysis shows that seven of nine agency participants were unable to provide an accurate and complete inventory of their web applications while one OIG used their agency's (agency 2) inventory due to the inability to conduct their own full inventory scan. An initial inventory request to the respective agencies produced an overall inventory of 584 public facing web applications. However, the work performed during Phase 1 identified a total of 1,004 public facing web applications, resulting in 420 unaccounted for applications. Figure 3 below shows the number of web applications the agencies provided versus what we found during the review. As a note, two agencies were not able to provide any inventory of their web applications (agencies 4 and 7). Also as seen in Figure 3, agency 9 had a large discrepancy between their documented inventory and what their OIG found.

Figure 3. Web application inventory results



8 of 9 agencies were not performing discovery scans

The possible cause for the inventory discrepancies may be attributed to the fact that eight of the nine participating agencies did not regularly perform discovery scans of their public facing network, which would have helped them to develop and maintain an accurate and complete inventory. IT environments are dynamic, with systems, hardware, and software frequently changing. Conducting regular discovery scans can detect new systems on the network and validate others that have been removed.

The OIGs generally found that their agencies' Office of the Chief Information Officer (OCIO) were not aware of all the web applications. OIGs discovered that web applications had been developed by agency subcomponents outside of the agency IT environment without the knowledge of the OCIO. The impact of this potential security issue was magnified by the fact that many of these applications contain Personally Identifiable Information (PII) and sensitive agency data. In fact, more than a fourth of the 1,004 web applications identified by the OIGs contained PII or sensitive data; 264 applications contained PII and 267 applications[9] contained agency sensitive data.[10] One agency was unable to determine how many of their applications contained PII or agency sensitive data.

Nearly a third of the identified web applications contained PII or Agency sensitive data

In addition to the lack of conducting discovery scans, inventory discrepancies generally occurred because either the agencies relied on manual reporting of the systems to a centralized office or agencies had a decentralized process that tasked the agency sub-components with being responsible for maintaining their own inventories. Additionally, the responses from the 22 OIGs were analyzed and determined that

81 percent of all agencies surveyed for this review did not maintain a comprehensive web application inventory

[9] In multiple instances, applications that contained PII also contained agency sensitive data. Therefore, the 267 applications that held agency sensitive data were not always additional applications.

[10] Sensitive data and information, per NIST, is any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovision that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order. Sensitive data or information can and often is categorized as Controlled Unclassified Information (CUI).

82 percent of those agencies did not maintain a comprehensive inventory. Including the nine agencies participating in this project, 81 percent of all agencies surveyed did not maintain a comprehensive web application inventory.

Without an accurate and complete inventory, which includes controlling and monitoring the number of applications, the agencies involved did not know the extent to which their data reside outside their own information system boundaries. This impacts an agency's implementation of effective patch management and data governance programs because those programs are often ineffective for unknown web application systems. Failure to maintain, control, and monitor an inventory of web applications increases the risk that applications could exist inside or outside an agency's network environment without the OCIO's knowledge. As a result, these applications may not be scanned, patched, or monitored as part of a continuous monitoring program. Conducting regularly scheduled network scans provide a method to validate current inventory and ensure no unapproved web applications reside in the IT environment.

Summary:

The Council on Cybersecurity[11] designated an inventory of hardware and an inventory of software as the top two critical security controls for building a secure network. Attackers are continuously scanning the address space of target organizations, waiting for new and unprotected systems to be attached to a network. Therefore, it is critical to maintain an asset inventory of all systems and applications the agencies administers. Without an accurate and complete inventory, agencies cannot ensure the appropriate controls are in place to protect the systems and their data.

INVENTORY REVIEW RECOMMENDATIONS

RECOMMENDATION 1

OMB should require Federal agencies to create and maintain a comprehensive inventory of web applications that will ensure consistency in implementation of security controls at the agency level. Agencies should include in their inventories the information below:

- Which applications are public facing;
- Which applications contain PII or sensitive agency information;
- Names of the application owners; and
- Descriptions of all system interfaces with each web application.

RECOMMENDATION 2

OMB should implement metrics to require agencies to report on:

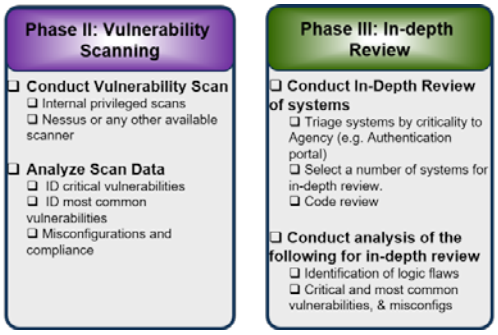
- Identifying and maintaining an updated inventory of public facing web applications;
- Developing an automated process to detect new web applications in the IT environment; and
- Implementing a process to ensure all web application changes in the IT environment have been authorized

[11] The Council on Cybersecurity is an independent, expert, not-for-profit global organization that was formed to maintain and make available effective cybersecurity controls, measures, policy, and best-business practice. The Council specifically maintains the Critical Security Controls (CSC), which have been recognized as the industry standard cybersecurity controls. The controls provide actionable measures to mitigate the most pervasive cyber-attacks.

VULNERABILITY REMEDIATION NEEDED (PHASES TWO & THREE)

Requirement:

Figure 4. Vulnerability and in-depth review phases



Our objectives for the vulnerability assessment phase were to (1) use automated tools to scan most of the hardware and software that supported applications identified during Phase 1 and (2) to conduct in-depth automated and manual testing on a sample of these applications (see Figure 4). The focus for the in-depth sample application testing was to detect security misconfigurations and known vulnerabilities on those systems with the highest agency risk. Finally, the results were compiled and grouped according to severity and web application flaw category using the NIST National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) (see Table 1) and OWASP Top Ten security flaw categories (see Table 2). The CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its model ensures repeatable accurate measurement using a standardized scoring system that allows an organization to prioritize the remediation of vulnerabilities based on risk. As stated previously in this report, OWASP is an open community that has created the OWASP Top Ten project to raise awareness about application security by identifying some of the most critical risks facing organizations. The OWASP Top Ten represents a broad consensus from security experts around the world on the most critical web application security flaws.

Table 1. CVSS Rating Scale

Severity	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Table 2. OWASP Top 10 Vulnerabilities

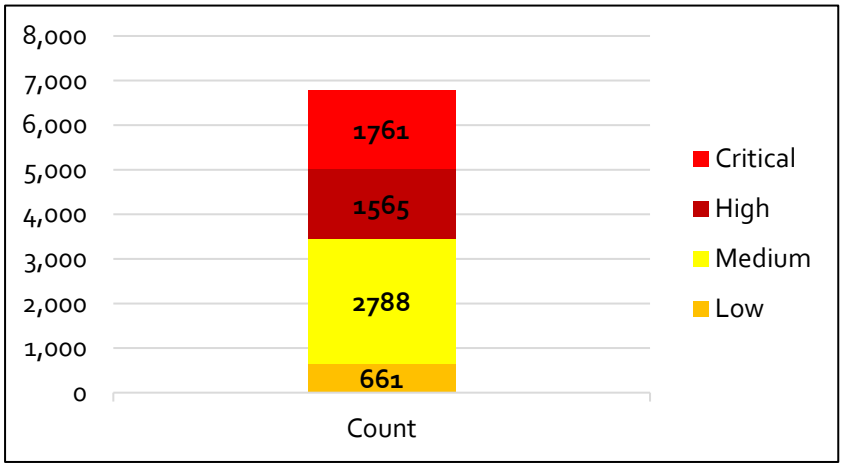
OWASP Top 10	
A1	Injection
A2	Broken Authentication and Session Management
A3	Cross-Site Scripting (XSS)
A4	Insecure Direct Object References
A5	Security Misconfiguration
A6	Sensitive Data Exposure
A7	Missing Function Level Access Control
A8	Cross-Site Request Forgery (CSRF)
A9	Using Known Vulnerable Components
A10	Unvalidated Redirects and Forwards

Results:

The vulnerability assessments identified thousands of vulnerabilities on the hardware and software supporting the applications identified in the inventory phase (Phase 1). Specifically, a total of 6,775 network level vulnerabilities (e.g. operating systems, web servers, application servers) ranging from low to critical severity were found within the nine agencies by performing internal[12] and external scans (see Figure 5). More importantly, 49 percent of the vulnerabilities identified were critical or high, having a CVSS score of at least 7.0 (See Figure 6). OIGs shared findings with their agencies through discussions and plan to include their findings in agency specific reports.

While it is up to each agency to devise its own remediation response time in accordance with NIST and risk management processes, the U.S. Department of Homeland Security (DHS) and OMB have issued guidance to mitigate high priority vulnerabilities within 30 days.[13] The CVSS scoring model allows prioritization of vulnerabilities according to severity and is a way for agencies to prioritize resources needed for remediation. Publicly accessible web applications and websites are often targets of malicious attacks. Therefore, it is a significant risk to have exploitable vulnerabilities on the supporting hardware and software of agency web applications.

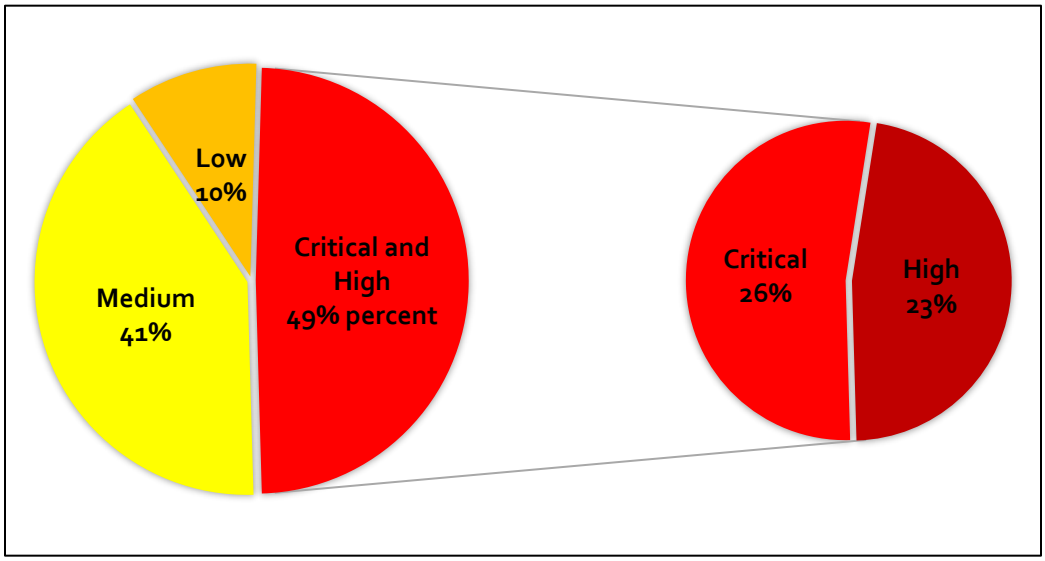
Figure 5. Count of vulnerabilities by severity



[12] Scans were conducted using a valid privileged account, often termed as credentialed scans. Credentialed scans are scans in which the scanning computer has an account on the computer being scanned that allows the scanner to do a more thorough check looking for problems that cannot be seen from the network (https://security.berkeley.edu/faq/nessus-network-vulnerability-scanning/how-do-i-run-credentialed-nessus-scan-windows-computer).

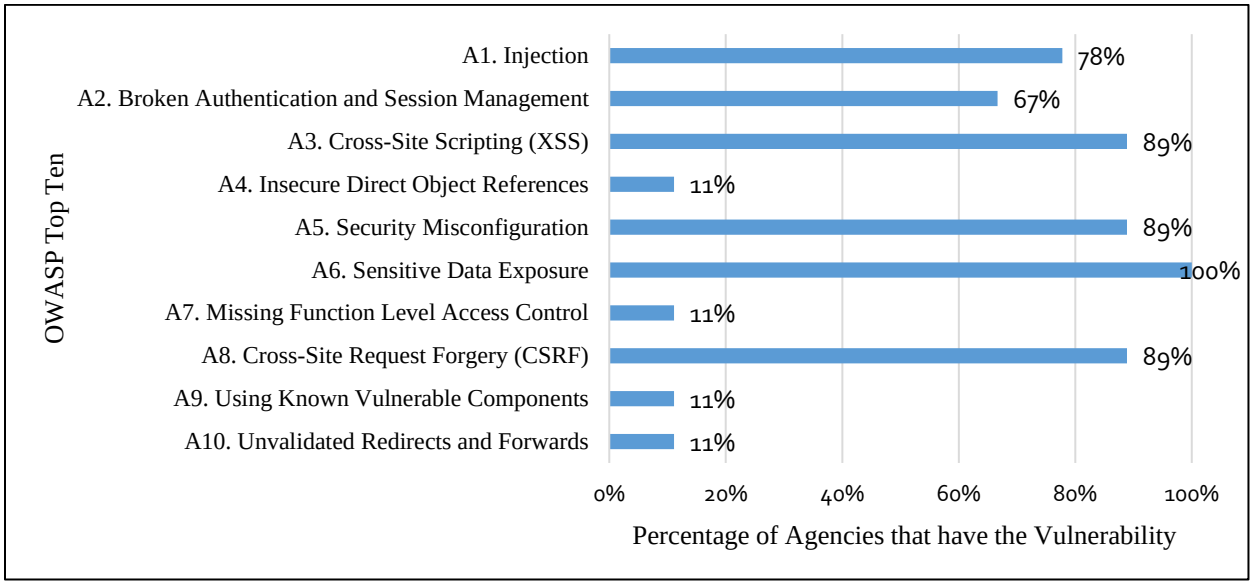
[13] Source: OMB M-17-09, Management of Federal High Value Assets.

Figure 6. Percent of vulnerabilities by severity



Additionally, the automated and manual in-depth review identified the existence of critical web application security flaws in Federal agency public websites in each of the OWASP Top Ten categories. Six out of the ten categories were identified in at least 67 percent of the nine agencies reviewed, with one of those present in all of the agencies' environments. The six categories were injection, broken authentication and session management, cross-site scripting, security misconfiguration, sensitive data exposure, and cross site request forgery, with sensitive data exposure present in all (see Figure 7). For example, some applications transmitted PII over unencrypted channels due to the use of insecure or outdated protocols. Others contained injection flaws that could lead to the unauthorized retrieval of agency sensitive data.

Figure 7. Percent of participating agencies with OWASP Top 10 flaws



These vulnerabilities can be attributed primarily to insufficient or ineffective policies and procedures related to the secure configuration and vulnerability management of web applications, including policies and procedures for hardening[14] web servers, secure programming, and integrating security into all phases of the software development life cycle. Additionally, some agencies did not have sufficient resources to identify and remediate web application vulnerabilities, while others had weaknesses in patch management procedures that contributed to the existence of vulnerabilities.

Summary:

Securing critical software resources is more important than ever as the focus of attackers has steadily moved toward vulnerabilities in the application. Government-wide, agencies reported incidents in fiscal year 2016 that showed that the web[15] was the third highest attack vector.[16] Additionally, effective vulnerability, configuration, and patch management, including secure hardening of servers and secure software development, can help mitigate well known vulnerabilities from being exploited via common attack vectors.

VULNERABILITY REVIEW RECOMMENDATIONS

RECOMMENDATION 3

OMB should implement metrics to require agencies to report on processes for automating assessments of system vulnerabilities using accounts with internal access and automating assessments of vulnerabilities in public facing web applications.

RECOMMENDATION 4

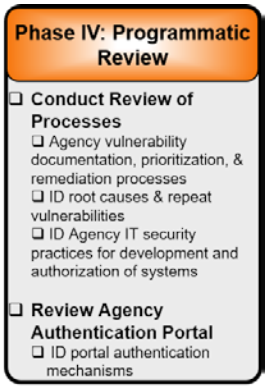
OMB should implement metrics to require agencies to report on the tracking, prioritization, and remediation of vulnerabilities in public facing web applications.

POLICES AND PROCEDURES TO SECURE WEBAPPLICATIONS ARE GENERALLY LACKING (PHASE FOUR)

Requirement:

The final phase of the project review was to conduct a programmatic assessment and analysis of processes and procedures used by the participating agencies to authorize and secure publicly accessible web applications. Examples of processes and procedures are vulnerability management documentation, prioritization and remediation processes, and any other IT security practices for the development, authorization, and secure configurations of web applications. Figure 8 illustrates the minimum requirements used by the participating OIGs for the programmatic assessment phase.

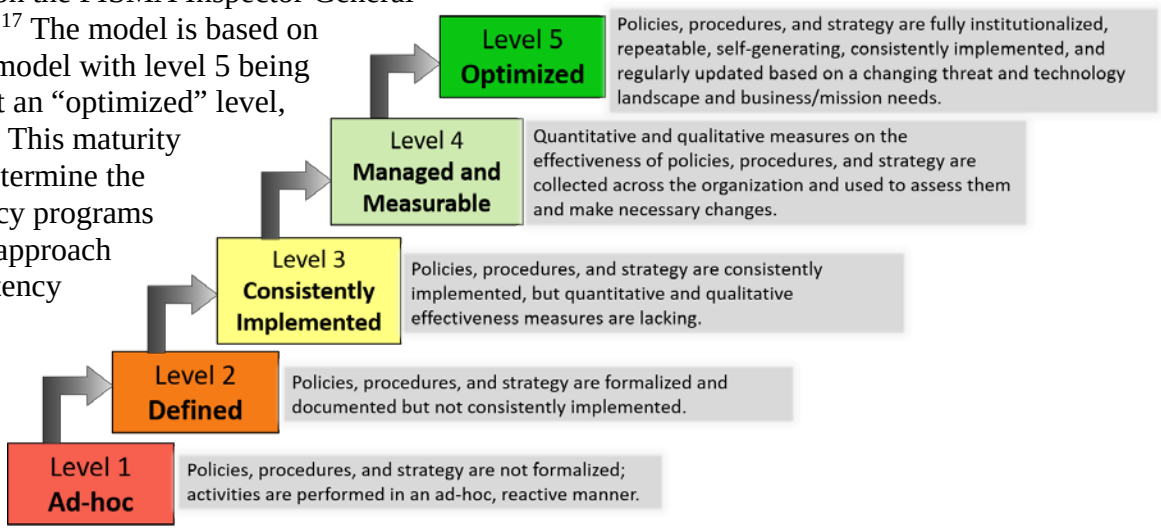
Figure 8. Programmatic Assessment Phase Requirements



[14] Hardening is the process of securing a system by reducing its surface of vulnerabilities.
[15] An attack executed from a website or web-based application.
[16] OMB, Federal Information Security Modernization Act of 2014, Annual Report to Congress, Fiscal Year 2016.

Based on the participants' results, most of the nine reviewed agencies were performing at a level 1 or level 2 maturity level based on the FISMA Inspector General (IG) Maturity Model.[17] The model is based on a five level maturity model with level 5 being the most mature, or at an "optimized" level, as shown in Figure 9. This maturity model was used to determine the effectiveness of agency programs using a standardized approach to help ensure consistency across the OIGs participating in this project.

Figure 9. IG maturity model level characteristics



The participating OIGs were able to gather data on seven distinct programmatic categories addressing web application processes and procedures for the development, operations, and security at the agencies. The categories are as follows:

- Overall web application security policies and procedures,
- Secure web application programing policies and procedures,
- Ability and procedures to secure the web application server operating environment,
- Systems development life cycle considerations capabilities and processes,
- Web application inventory processes,
- Account access and password procedures, and
- Web application consolidation efforts.

As stated in the Objective, Methodology, and Scope section of this report, detailed Phase 4 data was collected on eight of the nine agencies as 1 OIG did not complete a review of Phase 4. Also, high level data was collected on an additional 22 agencies and reported by their OIGs.

[17] The FISMA IG Maturity Model was a partnership between CIGIE, OMB, and DHS to move the IG assessment metrics to a maturity model approach. The maturity model allows the assessment of criteria, such as proper web application implementation, to be assessed based on the effectiveness of information security programs on a maturity model spectrum. The project team did not use the FISMA metrics from the FISMA IG Maturity Model but instead used the framework with specific web application criteria coming from OWASP and NIST. The maturity model used by the CIGIE project group portrays only a portion of the overall results in this report. Initially, the CIGIE Web Application Security Cross-Cutting project group used a similar Department of Defense capability maturity model (CMM), but the resulting data was translated to the IG maturity model due to the similarities. The project group used these models to determine the maturity of the development, operations, and maintenance of Agency publicly accessible web applications.

Results:

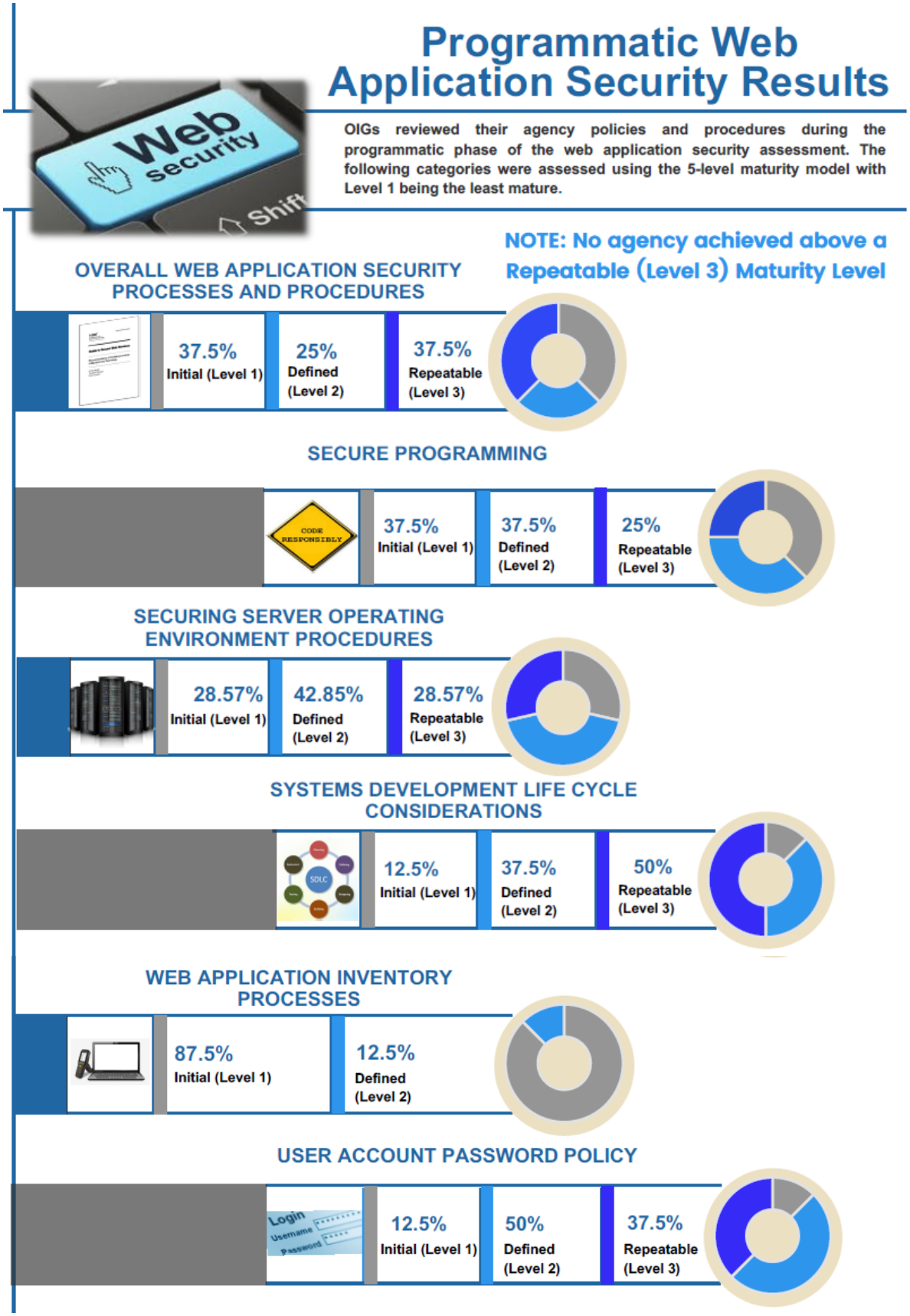
77 percent of agency results were at level 1 or 2 maturity level, resulting in ineffective security processes and procedures

Agency processes and policies were generally not documented or implemented to properly secure publicly accessible web applications in accordance with NIST and industry best practices, such as OWASP and the CIS critical security controls. As the data showed, the nine participating agencies were at a low maturity level for all of the reviewed programmatic factors. Using the maturity model described in Figure 9, 77 percent of the agencies were only at level 1 or level 2 maturity levels, and no results were higher than a level 3 out of the 5 levels of maturity. The OIGs found that the majority of the policies and procedures to secure web applications were not effective or did not specifically address web applications. Of specific concern is that 38 percent of the reviewed agencies were at only level 1 maturity for documentation and implementation of overall web based application security and secure programming of web applications policies and procedures.

Furthermore, when reviewing the capabilities of the participating agencies, it was found that half had deficiencies in the remediation of web application vulnerabilities. For example, one agency's OIG identified that four of nine vulnerabilities found remained uncorrected for longer than 90 days. Another agency had policies and procedures for correcting web application vulnerabilities but was not following them. The following figure shows the results of this data.

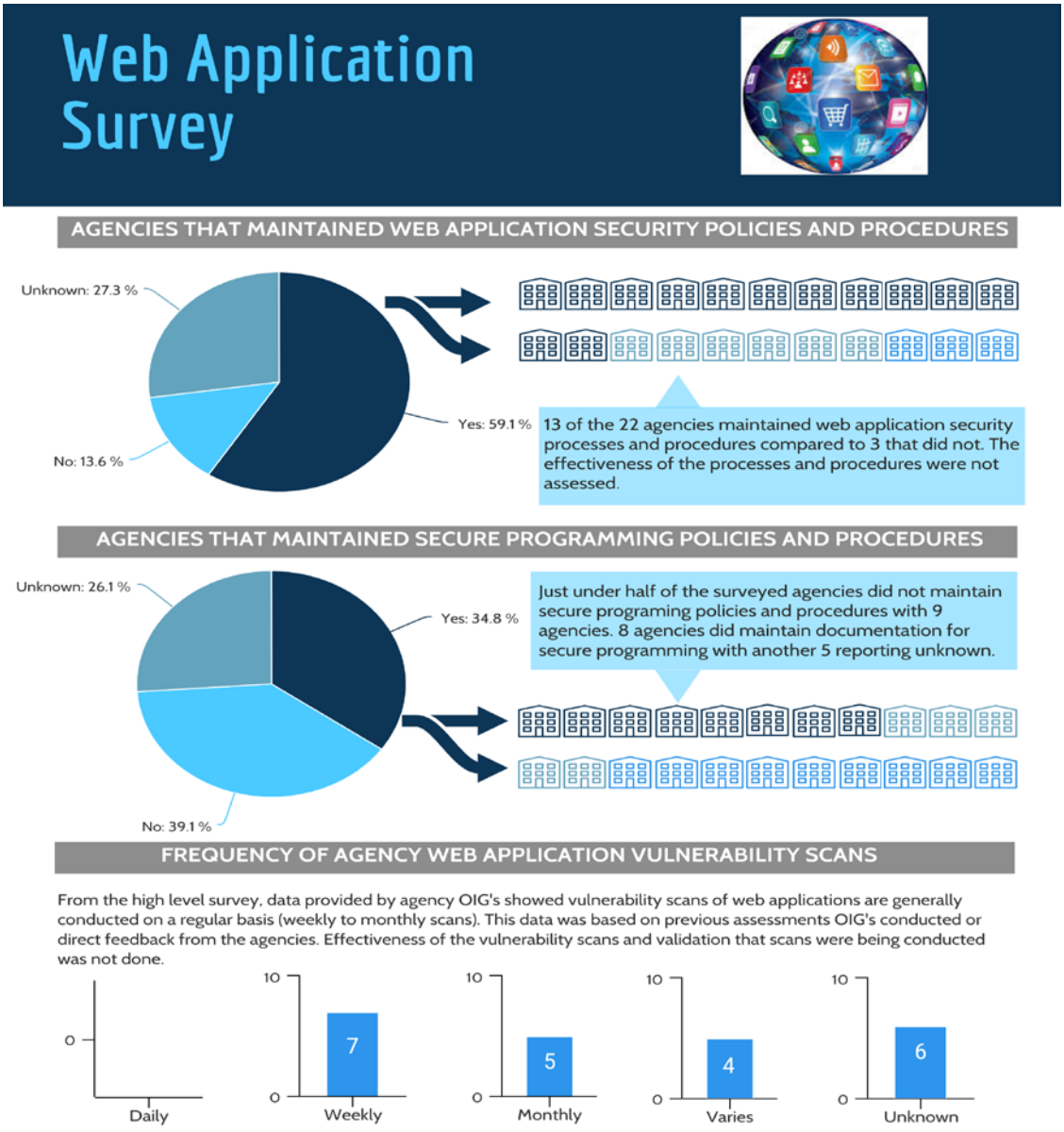
Half of the agencies did not have effective remediation capabilities

Figure 10. Phase four categories 1-6 data results



In addition to the nine OIGs participating in the detailed review and data collection of their agencies, another 22 OIGs responded to a high level web application security survey. The results for the high level programmatic questions asked of the additional 22 OIGs are below (Figure 11). The results were similar in that approximately 40 percent of agencies did not maintain or did not know if they maintained web application security policies and procedures. Additionally, approximately 65 percent of the 22 responding OIGs stated their agencies did not or did not know if their agencies implemented proper programming and procedural techniques to develop secure web applications.

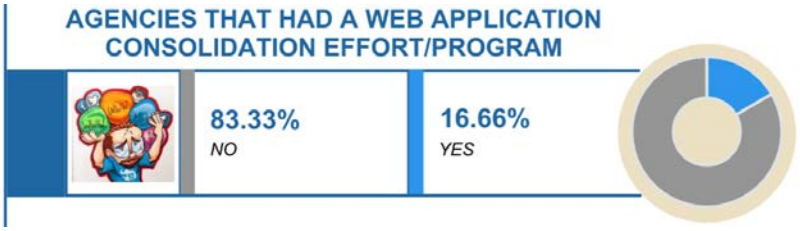
Figure 11. Phase four survey results from 22 additional agencies



The OIG participants also assessed whether their agencies conducted any web application consolidation efforts or maintained a web consolidation program. Although a consolidation effort is not required, it is a good practice to reduce redundancy and attack surface. For the nine agency participants, only one agency had a comprehensive program or process in place to control and reduce the number of web applications.

This was also prevalent in the wider OIG survey results, which showed that only 4 out of 22 agencies have a program in place to reduce the number of publicly accessible web applications.

Figure 12. Category 7 results, web application consolidation efforts



Providing relevant data and services to U.S. taxpayers is crucial in providing an open and honest government and should be done in accordance with current laws and regulations, such as the OPEN Government Data Act of 2002.[18] We believe that agencies should strive to consolidate web applications and websites to increase efficiency and reduce costs and efforts needed to secure and maintain agency assets and systems. Per OMB memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services*, public websites "are the primary means by which the public receives information from and interacts with the Federal Government." The memorandum also states that Federal Government websites are required to follow the same NIST and FISMA standards as all other Federal computer systems.

Summary:

The findings discovered during the programmatic phase show that improvements are needed in adequate centralization of policy, guidance, and enforcement of cybersecurity. Efforts for proper implementation and operations of many publicly accessible Federal Agency websites and applications could be improved. Without proper implementation of cybersecurity processes and procedures, based on sound risk management decisions, agency web applications and data continue to be at risk.

PROGRAMATIC REVIEW RECOMMENDATIONS

RECOMMENDATION 5

OMB should require Federal agencies review cybersecurity processes and procedures to ensure they cover web applications, to include:

- Incorporating NIST Special Publication 800-95, *Guide to Secure Web Services*, guidance in current and future cybersecurity processes and procedures;
- Comply with guidelines and requirements in OMB Memorandum M-17-06, *Policies for Federal Agency Public Websites and Digital Services*; and
- Using the previous stated guidance to ensure that policies and procedures address the secure configuration and vulnerability management of web servers and applications, including hardening web servers, securing programming, and integrating security into the software development lifecycle.

RECOMMENDATION 6

OMB should implement metrics to require agencies to report on web application consolidation processes that review the types of web applications to minimize redundancy and unnecessary public exposure.

[18] https://www.archives.gov/about/laws/egov-act-section-207.html

RECOMMENDATION 7

OMB should implement metrics to require agencies to report on remediation efforts that ensure critical and high-severity web application vulnerabilities are mitigated within required Federal and agency timelines. To help implement this recommendation, the following should be considered in guidance to agencies:

- Adding financial resources to ensure the proper tools and procedures are implemented and enforced;
- Increasing personnel subject matter expertise resources through training and proper hiring practices.

CONCLUSION

This project represented a broad section of the Federal Government, as the participants consisted of a blend of large, medium, and small agencies (see Appendix B). Federal agency publicly accessible web applications are top attack targets for malicious actors attempting to disrupt government operations or steal valuable and sensitive data. Based on the results of this project, publicly accessible web applications reviewed by the participating OIGs are generally at risk for being targeted. While web applications were only reviewed at nine agencies, the CIGIE project group revealed significant risks that could indicate a broader problem throughout the Federal Government. Furthermore, the 9 participating agencies and 22 survey respondents show that improvements are needed to develop a consistent and accurate inventory of web applications and effective vulnerability mitigation and patch management programs to ensure vulnerabilities and deficiencies are identified and promptly addressed. Also, improvements are needed in proper implementation of processes and procedures to enhance vulnerability management, a key to identifying and resolving security weaknesses. This report shows that it is imperative that Federal agencies find and mitigate, if they have not already, vulnerabilities in web applications and be provided the resources to do this before more attackers can exploit those vulnerabilities. OCIO's need to have proper oversight authority and support from the agency to implement the recommendations and best business practices provided in this report.

Appendix A – List of Acronyms

Acronym	Definition
DHS	U.S. Department of Homeland Security
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIS	Center for Internet Security
CMM	Capability Maturity Model
CVSS	Common Vulnerability Scoring System
HUD	U.S. Department of Housing and Urban Development
FISMA	Federal Information Security Modernization Act
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	U.S. Office of Management and Budget
OWASP	Open Web Application Security Project
PII	personally identifiable information

Appendix B – List of Participating Office of Inspectors General and Associated Agencies by Agency Type

Nine participating agencies:

- Cabinet level agencies: 3
- Large non-cabinet agencies: 1
- Midsize agencies: 3
- Small agencies: 0
- Other type of agencies: 2

All participating agencies (includes the 9 above and the 22 survey respondents):

- Cabinet level agencies: 9
- Large non-cabinet agencies: 2
- Midsize agencies: 9
- Small agencies: 7
- Other type of agencies: 4