Bureau of Consumer Financial Protection
1700 G Street NW
Washington, D.C. 20552

May 7, 2020

The Honorable Patrick McHenry
Ranking Member
Committee on Financial Services
U.S. House of Representatives
4340 O'Neill House Office Building
Washington, DC 20024

Dear Ranking Member McHenry:

Thank you for your letter of April 22, 2020, regarding the Consumer Financial Protection Bureau's (Bureau's) efforts related to cybersecurity, particularly in light of the COVID-19 pandemic. The Bureau recognizes the importance of cybersecurity of both the financial industry and our own internal information systems, and we are working alongside fellow state and federal regulatory entities, as well as supervised institutions, to ensure we remain current with the changing threat landscape.

The Bureau is a member of the Financial and Banking Information Infrastructure Committee (FBIIC). Chaired by the Department of Treasury, the FBIIC is charged with improving coordination and communication among financial regulators, promoting public-private partnerships within the financial sector, and enhancing the resiliency of the financial sector overall. With respect to cybersecurity, the FBIIC coordinates inter-agency cybersecurity policy developments, including strengthening information sharing on cyber vulnerabilities, threats, and incidents; furthering the adoption of cybersecurity best practices; and enhancing the financial sector's ability to respond to and recover from cyber incidents.

The Bureau is also a member of the Federal Financial Institutions Examination Council's (FFIEC's) Cybersecurity and Critical Infrastructure Working Group (CCIWG). Through the CCIWG, the Bureau works with other financial regulators to develop standardized examinations procedures which can inform regulated institutions of best practices during a heightened level of cybersecurity awareness. As you may know, the FFIEC recently issued a joint statement to address the use of cloud computing services and security risk management principles in the financial services sector. A copy of the joint statement is enclosed with this letter.

With respect to your specific questions: to date, the Bureau is not aware of any cyberattacks perpetrated against financial services entities related to COVID-19. Nor is the Bureau aware of any change in the frequency of such attacks as a result of the COVID-19 pandemic. It is important to note that while the Bureau does have certain authorities related to cybersecurity, Congress specifically excluded important statutory provisions related to data security from the Bureau's purview. For example, the Bureau does not have any authority to supervise for, enforce compliance with, or write regulations implementing the Gramm-Leach-Bliley Act's safeguards provision or the Fair Credit Reporting Act's records disposal provision. And while the Bureau receives regular updates from the FBIIC on suspected and actual cyber incidents, entities subject to the Bureau's supervisory authority are not required to notify the Bureau of suspected or actual cyber incidents.

As it relates to the cybersecurity of the Bureau's own information systems, the Bureau continues to proactively monitor those systems for anomalies or indicators of compromise. The Bureau also coordinates closely with law enforcement and national security agencies to monitor cyber threats and to take appropriate action. If any hack or advanced persistent threat penetrates the Bureau's first layer of defense, our automated detection capabilities would notify the Bureau's Cybersecurity Incident Response Team (CSIRT), which would then work with the United States Computer Emergency Readiness Team and the Department of Homeland Security to respond appropriately. While there has been an increase in the number of attempted cyberattacks on the Bureau's internal systems since January 2020, none has been successful.

Nevertheless, the Bureau continues to prioritize development of new systems, tools, and procedures to improve its cybersecurity program with a focus on risk management and protection of sensitive data. For example, the Bureau has published enhanced guidance for its employees for acceptable cybersecurity practices on third-party teleconference platforms; integrated increased malware protection at network gateways, on laptops, on servers, as well as in cloud services; and increased the frequency of cybersecurity awareness bulletins, advisories, and communications distributed to all staff as new information becomes relevant to the workforce. Enclosed is a copy of the enhanced guidance for acceptable cybersecurity practices on third-party teleconference platforms and the numerous cybersecurity awareness communications to staff since January 21, 2020.

Additionally, the Bureau's Office of Inspector General (OIG) conducts a yearly audit of the Bureau's information security program. In its most recent audit, the OIG concluded that the Bureau's information security continuous monitoring process and incident response process are effective. Enclosed is a copy of the OIG's report from that audit.

Should you have any questions about this response, please do not hesitate to contact me, or have your staff contact Kate Fink of the Bureau's Office of Legislative Affairs. Ms. Fink can be reached at (b) (6) [redacted]

Sincerely,

Kathleen L Kraninger

Kathleen L. Kraninger
Director

Enclosure

cc: The Honorable Maxine Waters, Chairwoman, Committee on Financial Services

Federal Financial Institutions Examination Council

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • www.ffiec.gov

Joint Statement

Security in a Cloud Computing Environment

INTRODUCTION

The Federal Financial Institutions Examination Council (FFIEC) on behalf of its members[1] is issuing this statement to address the use of cloud computing[2] services and security risk management principles in the financial services sector. Financial institution management should engage in effective risk management for the safe and sound use of cloud computing services. Security breaches involving cloud computing services highlight the importance of sound security controls and management's understanding of the shared responsibilities between cloud service providers and their financial institution clients.

This statement does not contain new regulatory expectations; rather, this statement highlights examples of risk management practices for a financial institution's safe and sound use of cloud computing services and safeguards to protect customers' sensitive information from risks that pose potential consumer harm. Management should refer to the appropriate FFIEC member guidance referenced in the "Additional Resources" section of this statement for information regarding supervisory perspectives on effective information technology (IT) risk management practices. This statement also contains references to other resources, including the National Institute of Standards and Technology (NIST), National Security Agency (NSA), Department of Homeland Security (DHS), International Organization for Standardization (ISO), Center for Internet Security (CIS), and other industry organizations (e.g., Cloud Security Alliance).

BACKGROUND

Due diligence and sound risk management practices over cloud service provider relationships help management verify that effective security, operations, and resiliency controls are in place and consistent with the financial institution's internal standards. Management should not assume that effective security and resilience controls exist simply because the technology systems are operating in a cloud computing

[1] The FFIEC comprises the principals of: the Board of Governors of the Federal Reserve System, Bureau of Consumer Financial Protection, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and State Liaison Committee.

[2] NIST SP 800-145, *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*, defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or third-party service provider interaction.

environment. The contractual agreement between the financial institution and the cloud service provider should define the service level expectations and control responsibilities for both the financial institution and provider. Management may determine that there is a need for controls in addition to those a cloud service provider contractually offers to maintain security consistent with the financial institution's standards.

Ongoing oversight and monitoring of a financial institution's cloud service providers are important to gain assurance that cloud computing services are being managed consistent with contractual requirements, and in a safe and sound manner. This oversight and monitoring can include evaluating independent assurance reviews (e.g., audits, penetration tests, and vulnerability assessments), and evaluating corrective actions to confirm that any adverse findings are appropriately addressed. Risk management expectations for the management of relationships involving third parties (such as third-party cloud computing services) are outlined in FFIEC members' respective guidance and the Information Security Standards.[3]

Cloud computing environments are enabled by virtualization[4] technologies, which allow cloud service providers to segregate and isolate multiple clients on a common set of physical or virtual hardware. Financial institutions use private cloud computing environments,[5] public cloud computing environments,[6] or a hybrid of the two. NIST generally defines three cloud service models.[7] For each service model, there are typically differing shared responsibilities between the financial institution and the cloud service provider for implementing and managing controls. These models and the typical responsibilities include:

- **Software as a Service (SaaS)** is similar to traditional outsourcing in which the software applications (applications) operate on the provider's cloud infrastructure. In this model, financial institution management does not typically manage, maintain, or control the underlying cloud infrastructure or individual application capabilities. The financial institution is responsible for user-specific application configuration settings, user access and identity management, and risk management of the relationship with the cloud service provider. The cloud service provider is responsible for any changes to and maintenance of the applications and infrastructure.

- **Platform as a Service (PaaS)** is a model in which a financial institution deploys internally developed or acquired applications using programming languages, libraries, services, and tools supported by the cloud service provider. These applications reside on the provider's platforms

[3] A financial institution's overall information security program must also address the specific information security requirements applicable to "customer information" set forth in the "Interagency Guidelines Establishing Information Security Standards" implementing section 501(b) of the Gramm–Leach–Bliley Act and section 216 of the Fair and Accurate Credit Transactions Act of 2003. See 12 CFR 30, appendix B (OCC); 12 CFR part 208, appendix D-2, and 12 CFR part 225, appendix F (FRB); 12 CFR 364, appendix B (FDIC); and 12 CFR 748, appendix A (NCUA) (collectively referenced in this statement as the "Information Security Standards").
[4] The NIST Glossary defines virtualization as the simulation of the software and/or hardware upon which other software runs.
[5] The NIST Glossary defines private cloud computing as "The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises."
[6] The NIST Glossary defines public cloud computing as "The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider."
[7] NIST SP 800-145, The NIST Definition of Cloud Computing.

and cloud infrastructure. PaaS models necessitate similar risk management as the SaaS model. However, management is also responsible for appropriate provisioning and configuration of cloud platform resources and implementing and managing controls over the development, deployment, and administration of applications residing on the provider's cloud platforms. The cloud service provider is responsible for the underlying infrastructure and platforms (including network, servers, operating systems, or storage).

- **Infrastructure as a Service (IaaS)** is a model in which a financial institution deploys and operates system software, including operating systems, and applications on the provider's cloud infrastructure. Like PaaS, the financial institution is responsible for the appropriate provisioning and configuration of cloud platform resources and implementing and managing controls over operations, applications, operating systems, data, and data storage. Management may need to design the financial institution's systems to work with the cloud service provider's resilience and recovery process. Also, as in the other models, the financial institution is responsible for risk management of the relationship with the cloud service provider. The cloud service provider is responsible for controls related to managing the physical data center. For example, the cloud service provider updates and maintains the hardware, network infrastructure, environmental controls (e.g., heating, cooling, and fire and flood protection), power, physical security, and data communications connections. Additionally, cloud service providers are typically responsible for managing the hypervisor(s).[8]

These examples describe typical shared responsibilities for the different service models; however, the specific services and responsibilities will be unique to each service deployment and implementation. Regardless of the environment or service model used, the financial institution retains overall responsibility for the safety and soundness of cloud services and the protection of sensitive customer information.[9]

RISKS

In cloud computing environments, financial institutions may outsource the management of different controls over information assets and operations to the cloud service provider. Careful review of the contract between the financial institution and the cloud service provider along with an understanding of the potential risks is important in management's understanding of the financial institution's responsibilities for implementing appropriate controls. Management's failure to understand the division of responsibilities for assessing and implementing appropriate controls over operations may result in increased risk of operational failures or security breaches. Processes should be in place to identify, measure, monitor, and control the risks associated with cloud computing. Failure to implement an effective risk management process for cloud computing commensurate with the level of risk and complexity of the financial institution's operations residing in a cloud computing environment may be an unsafe or unsound practice and result in potential consumer harm by placing customer-sensitive information at risk.

[8] NIST defines a hypervisor as the virtualization component that manages the guest operating systems (OSs) on a host and controls the flow of instructions between the guest OSs and the physical hardware. A function of the hypervisor is to logically separate virtual machines from each other in the virtual network.

[9] *See* the Information Security Standards:12 CFR 30, appendix B (OCC); 12 CFR part 208, appendix D-2, and 12 CFR part 225, appendix F (FRB); 12 CFR 364, appendix B (FDIC); and 12 CFR 748, appendix A (NCUA).

RISK MANAGEMENT

Examples of relevant risk management practices for assessing risks related to and implementing controls for cloud computing services include:

Governance

- **Strategies for using cloud computing services as part of the financial institution's IT strategic plan and architecture.** The financial institution's plans for the use of cloud computing services should align with its overall IT strategy, architecture, and risk appetite. This includes determining the appropriate level of governance, the types of systems and information assets considered for cloud computing environments, the impact on the financial institution's architecture and operations model, and management's comfort with its dependence on and its ability to monitor the cloud service provider.

Cloud Security Management

- **Appropriate due diligence and ongoing oversight and monitoring of cloud service providers' security.** As with all other third-party relationships, security-related risks should be identified during planning, due diligence, and the selection of the cloud service provider. Management should implement appropriate risk management and control processes to mitigate identified risks once an agreement is in place. The process for risk identification and controls effectiveness may include testing or auditing, if possible, of security controls with the cloud service provider; however, some cloud service providers may seek to limit a financial institution's ability to perform their own security assessment due to potential performance impacts. Management can leverage independent audit results from available reports (e.g., system and organizational control[10] (SOC) reports). Additionally, management can use the security tools and configuration management capabilities provided as part of the cloud services to monitor security. While risks associated with cloud computing environments are typically similar to traditional outsourcing arrangements, there are often key security considerations and controls that are unique to cloud computing environments.

- **Contractual responsibilities, capabilities, and restrictions for the financial institution and cloud service provider.** Contracts between the financial institution and cloud service provider should be drafted to clearly define which party has responsibilities for configuration and management of system access rights, configuration capabilities, and deployment of services and information assets to a cloud computing environment, among other things. When defining responsibilities, management should consider management of encryption keys, security monitoring, vulnerability scanning, system updates, patch management, independent audit requirements, as well as monitoring and oversight of these activities and define responsibility for these activities in the contract. Management should also consider operational resilience capabilities, incident response obligations, notification or approval requirements for the use of subcontractors (i.e., fourth parties), data ownership, expectations for removal and return of data

[10] Developed by the AICPA, system and organization controls (SOC) reviews refer to the audits of system-level controls of a third-party service provider.

at contract termination, and restrictions on the geographic locations where the financial institution's data may reside.

- **Inventory process for systems and information assets residing in the cloud computing environment.** An effective inventory process for the use of cloud computing environments is an essential component for secure configuration management, vulnerability management, and monitoring of controls. Processes to select and approve systems and information assets that are placed in a cloud computing environment should be established to ensure that risks are appropriately considered. An inventory management process to track systems and information assets residing in the cloud computing environment, including virtual machines, application programming interfaces, firewalls, and network devices can allow management to better manage and safeguard information assets.

- **Security configuration, provisioning, logging, and monitoring.** Misconfiguration of cloud resources is a prevalent cloud vulnerability and can be exploited to access cloud data and services.[11] System vulnerabilities can arise due to the failure to properly configure security tools within cloud computing systems. Financial institutions can use their own tools, leverage those provided by cloud service providers, or use tools from industry organizations to securely configure systems, provision access, and log and monitor the financial institution's systems and information assets residing in the cloud computing environment. Cloud computing may involve different security control configurations and processes than those employed in more traditional network architectures. Regardless of the configurations, tools, and monitoring systems employed, a key consideration is the regular testing of the effectiveness of those controls to verify that they are operating as expected. Management can use available audit or assurance reports to validate that testing is performed. Management may consider leveraging cloud computing standards and frameworks from industry standard-setting organizations to assist in designing a secure cloud computing environment while considering risk.[12]

- **Identity and access management and network controls.** Common practices for identity and access management for resources using cloud computing infrastructures include limiting account privileges, implementing multifactor authentication, frequently updating and reviewing account access, monitoring activity, and requiring privileged users to have separate usernames and passwords for each segment of the cloud service provider's and financial institution's networks. Default access credentials should be changed, and management should be aware of the risk of overprovisioning access credentials. Access to cloud tools for provisioning and developing systems, which may contain sensitive or critical bank-owned data should be limited. Examples of network controls include virtual private networks, web application firewalls, and intrusion detection systems. Management should consider implementing tools designed to detect security misconfigurations for identity and access management and network controls.

- **Security controls for sensitive data.** Controls (e.g., encryption, data tokenization,[13] and other

[11] In the National Security Agency's "Mitigating Cloud Vulnerabilities," the report notes that misconfigurations of cloud resources include policy mistakes, a misunderstanding of responsibility and inappropriate security controls.
[12] For example, refer to NIST's Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014.
[13] Data tokenization refers to the practice of substituting sensitive data with a random value, or token that is associated with the sensitive data.

data loss prevention tools) to safeguard sensitive data limit a malicious actor’s ability to exploit data during a breach. When using data encryption controls in a cloud computing environment, management should consider defining processes for encryption key management between the financial institution and the cloud service provider. Many cloud service providers offer cloud-based key management services, which allows integration with other cloud-based services. However, cloud-based key management services may allow administrators from a cloud service provider to access encrypted information. For this reason, management may elect to use the financial institution’s own encryption and key management services. The trade-off is that non-cloud-based encryption should be built into the application to work properly and application-based encryption may impede automated controls offered by cloud service providers. Common methods to manage encryption in cloud computing environments include the use of hardware security modules,[14] virtual encryption tools, cloud-based security tools, or a combination of these.

- **Information security awareness and training programs.** Training promotes the ability of staff to effectively implement and monitor necessary controls in the cloud computing environment. A wide range of resources are generally available to management, including information and training obtained from external, independent organizations on the use of cloud technologies. Management may also consider using product-specific training provided by cloud service providers to educate staff on product-specific security tools.

Change Management

- **Change management and software development life cycle processes.** Change management controls are important for effectively transitioning systems and information assets to a cloud computing environment. Management may augment existing change management processes and the software development life cycle (SDLC), as applicable, for cloud computing environments.

- **Microservice[15] architecture.** Though not unique to cloud application development, cloud implementation often uses microservices to develop applications with smaller, lighter-weight code bases that facilitate faster, more agile application development. However, there are security, reliability, and latency issues with microservices, and having multiple microservices can increase the financial institution’s attack surface.[16] Management should evaluate implementation options that meet the institution’s security requirements.

Resilience and Recovery

- **Business resilience and recovery capabilities.** Operations moved to cloud computing environments should have resilience and recovery capabilities commensurate with the risk of the service or operation for the financial institution. Management should review and assess the resilience capabilities and service options available from the cloud service provider. There may

[14] A hardware security module is a physical computing device that implements security functions, including cryptographic algorithms and key generation.

[15] NIST Glossary defines a microservice as a set of containers that work together to compose an application.

[16] *NIST Special Publication 800-204 Security Strategies for Microservices-based Application Systems* provides additional technical details for financial institutions considering the use of microservices.

be several configurations available, and management should determine which options best meet the institution's resilience and recovery requirements. Resilience and recovery capabilities are not necessarily included in cloud service offerings; therefore, the contract should outline the resilience and recovery capabilities required by the institution. Based on the cloud service model used, management should evaluate and determine how cloud-based operations affect both the business continuity plan and recovery testing plans. As with other operations, management should regularly update business continuity plans to reflect changes to configurations and operations and regularly test and validate resilience and recovery capabilities. Testing may need to be conducted jointly with the provider depending on the service model being used.

- **Incident response capabilities.** The financial institution's incident response plan should take into account cloud-specific challenges due to ownership and governance of technology assets owned or managed by the cloud service provider. The contract should define responsibilities for incident reporting, communication, and forensics. Cloud usage presents unique forensic issues related to jurisdiction, multi-tenancy, and reliance on the cloud service provider for a variety of forensic activities. Additionally, the service level agreement should identify specific activities for incident response and identify the cloud service provider's responsibilities in the event of an incident. When responding to an incident, management should recognize shared responsibilities and corresponding duties. Often, cloud service providers offer a variety of monitoring and alerting tools that can be leveraged by a financial institution and integrated into its incident response plans.

Audit and Controls Assessment

- **Regular testing of financial institution controls for critical systems.** Processes should be in place for regular audit and testing of security controls and configurations commensurate with the risk of the operations supported by the cloud service. These processes can include the audit and testing of the financial institution's security configurations and settings, access management controls, and security monitoring programs.

- **Oversight and monitoring of cloud service provider-managed controls.** Management should evaluate and monitor the cloud service provider's technical, administrative, and physical security controls that support the financial institution's systems and information assets that reside in the cloud environment. Oversight and monitoring activities include requesting, receiving, and reviewing security and activity reports from the cloud service provider; reports of compliance with service level agreements; product validation reports; and reports of independent assurance reviews (e.g., audits, penetration tests, and vulnerability assessments) performed on the cloud computing services. Other considerations may include personnel controls (e.g., background checks and security awareness training) for staff that supports the financial institution's operations or has access to financial institution data. Management may test the cloud service provider's controls if permitted by the contract. Where there is a limited ability to directly monitor or test the security controls managed by the cloud service provider, management may obtain SOC reports, other independent audit reports, or ISO certification reports to gain assurance that the controls are implemented and operating effectively. Management should understand the scope of independent assurance testing to determine whether the scope is comprehensive and the reports contain sufficient information for management to evaluate the cloud computing services.

- **Controls unique to cloud computing services.** While many of the controls outlined in this statement also apply to more traditional network architectures, there are controls unique to the architectures of cloud computing services. Examples of such controls include:
    - **Management of the virtual infrastructure.** The ability to create secure virtual infrastructures is managed through cloud security tools, such as the hypervisor, and should be closely controlled by the cloud service provider. The cloud service provider should be able to provide assurance that it has appropriate controls over the hypervisor, or other virtual infrastructure controls, to manage the cloud services being provided to the financial institution. For example, management should consider verifying whether cloud service providers scan their hypervisor code for vulnerabilities and monitor system logs. This can be accomplished by management or through reviews of available third-party assurance reports.
    - **Use of containers[17] in cloud computing environments.[18]** The advantages of using containers in a cloud-computing environment include portability and less memory utilization compared to using separate virtual machines (VMs). However, "[w]hile containers provide a strong degree of isolation, they do not offer as clear and concrete of a security boundary as a VM. Because containers share the same kernel and can be run with varying capabilities and privileges on a host, the degree of segmentation between them is far less than that provided to VMs by a hypervisor."[19] Therefore, when using containers, management should consider:
        - Storing data outside of the container, so that data do not have to be re-created when updating and replacing containers.
        - Verifying that configurations prevent containers from unintentionally interacting.
        - Securing containers from applications within them.
        - Securing the host from containers and vice versa.
        - Monitoring containers for vulnerabilities and updating or replacing containers when appropriate.

      Additionally, traditional security controls, such as firewalls and intrusion detection systems, may not be effective because containers may obscure activities; therefore, container-specific security solutions should be implemented.
    - **Use of managed security services for cloud computing environments.** Financial institutions may choose to leverage available security tools and services to assist with managing and monitoring security for cloud computing services. Common tools and services include use of cloud access security broker (CASB)[20] tools. For more information on managed security service providers, refer to "Outsourcing Technology

[17] NIST Glossary defines containers as a method for packaging and securely running an application within a virtualized environment. *NIST SP 800-190 Application Container Security Guide* states "The term is meant as an analogy to shipping containers, which provide a standardized way of grouping disparate contents together while isolating them from each other."
[18] *NIST Special Publication 800-190 Application Container Security Guide* provides additional technical details for financial institutions considering the use of containers.
[19] *NIST SP 800-190 Application Container Security Guide*.
[20] Cloud access security brokers are generally products or services that monitor activity between cloud service users and cloud applications and can typically be used to enforce security policies, alert for anomalous activity or monitor performance.

Services – Appendix D" of the *FFIEC IT Examination Handbook.*

- **Consideration of interoperability[21] and portability[22] of data and services.** When selecting or designing and building cloud computing services, management may consider interoperability and portability in the design of those services or application providers. A financial institution's interoperability and portability strategy will depend on the institution's risk appetite and the contracted service model (e.g., SaaS, PaaS, or IaaS) employed. Management may consider these capabilities as part of the initial contracting and design of cloud computing services.
- **Data destruction or sanitization.** Institutions should be aware of the processes that the cloud service provider uses for data destruction. The service level agreement should outline that adequate measures are taken to ensure data destruction is done in a manner that would prevent unauthorized disclosure of information.

ADDITIONAL RESOURCES

The risk management considerations outlined in this statement provide a summary of key controls that management may consider as part of assessing and implementing cloud computing services. However, specific risk management and controls will be dependent on the nature of the outsourced services and the specifics of the cloud implementation. Additional information on general third-party risk management and outsourcing practices is available in the *FFIEC Information Technology Examination Handbook's* "Outsourcing Technology Services" booklet and other documents published by FFIEC members.

There are also many industry-recognized standards and resources that can assist financial institutions with managing cloud computing services. Examples of these include NIST, the Center for Internet Security's Critical Security Controls, and the Cloud Security Alliance. Management may research and consider consulting industry-recognized standards and resources when developing and implementing security controls in a cloud computing environment.

[21] NIST 500-291, version 2: *NIST Cloud Computing Standards Roadmap* defines interoperability as the capability of data to be processed by different services on different cloud systems through common specifications.

[22] NIST 500-291, version 2: *NIST Cloud Computing Standards Roadmap* defined portability the ability for data to be moved from one cloud system to another or for applications to be ported and run on different cloud systems at an acceptable cost.

REFERENCES

U.S. Government Resources

FFIEC

FFIEC Information Technology Examination Handbook

FFIEC “Outsourced Cloud Computing” (July 10, 2012)

National Institute of Standards and Technology

NIST 800-144: Guidelines on Security and Privacy in Public Cloud Computing

NIST 800-145: The NIST Definition of Cloud Computing

NIST 800-146: Cloud Computing Synopsis and Recommendations

NIST 800-125: Guide to Security for Full Virtualization Technologies

NIST 800-125A Rev.1: Security Recommendations for Server-based Hypervisor Platforms

NIST Special Publication 800-125B: Secure Virtual Network Configuration for Virtual Machine (VM) Protection

NIST Special Publication 800-190: Application Container Security Guide

National Security Agency

Mitigating Cloud Vulnerabilities

Department of Homeland Security CISA

Microsoft Office 365 Office Security Observations

Cloud Security Guidance

The Basics of Cloud Computing

General Services Administration

Federal Risk and Authorization Management Program (FedRAMP)

Industry Resources

Center for Internet Security (CIS) Controls v.7 (Control 7)

Cloud Security Alliance

Institute of Electrical and Electronics Engineers (IEEE) Cloud Computing Standards

International Organization for Standardization (ISO)

OWASP

Number	Date	Organization
COO-T&I-01-2020	April 20, 2020	CFPB

Teleconference Participation Directive (TPD)

I. Overview

Federal law[1] mandates that all Federal data be safeguarded from unauthorized disclosure in any form. The Bureau employs a varied methodology to ensure CFPB data is protected across all technology platforms and services offered to its users. As these platforms and services become increasingly virtual, the Bureau has established policies, controls, and procedures to ensure data is protected in these virtual environments.

This directive applies to all Bureau employees and contractors who have access to Bureau data and who are responsible for protecting Bureau information and information systems. All information received by the Bureau is assigned a sensitivity level (Public, Low, Medium, or High). The sensitivity level can be based on a number of factors, but is primarily determined by:

- The authority under which the information was received
- Legal restrictions related to the information
- Any contractual restrictions, such as memoranda of understanding (MOUs), non-disclosure agreements, contracts, etc.

Individuals who violate this directive are subject to penalties that can be imposed under existing policy[2] and regulations.

II. Purpose

This directive establishes uniform guidance on CFPB user conduct when participating in teleconferences or virtual meetings hosted through CFPB platforms (e.g., CFPB Skype, CFPB Teams, CFPB Office 365, CFPB WebEx), or originated by third parties on platforms not authorized by CFPB (e.g., Zoom, GoToMeeting, etc.).

This directive supplements the Acceptable Use Policy (AUP)[3] and other CFPB policies that define appropriate use of CFPB technology assets, including the CFPB Information Sensitivity Leveling Standard, which defines important rules, guidelines, and expectations around the storage, access, use, and disclosure of information.

- Presence and sensitivity of Personally Identifiable Information (PII) or Direct Identifiers, or level of re-identification risk
- The commercial sensitivity of the information

[1] Refer to Section 5 for complete list of legal authorities

[2] Includes, but not limited to, disciplinary actions defined in the Bureau Disciplinary and Adverse Action Policy

[3] Reference Acceptable Use Policy

- Whether the information is available to the general public
- Bureau policy considerations arising from the content of the information[4]

III. Definitions

(b) (5) definitions of Public, Low, Medium, and High sensitivity data[5]

IV. Directive

The Teleconference Participation Directive (TPD) establishes uniform guidance on CFPB user conduct when participating in virtual meetings originated through CFPB platforms (e.g., CFPB Skype, CFPB Office 365, and CFPB WebEx) or by third parties. The Bureau may supplement the TPD with additional policy, directives, guidelines, and procedures, as appropriate. This TPD and any related implementing documents shall be reviewed and updated as needed to maintain relevance and alignment to federal policy and doctrine.[6]

1. Use of Third-Party-Originated Teleconferences/Virtual Meeting Applications
   CFPB users are permitted to join virtual meetings originated by third-paries and external applications, however, these channels shall be treated as insecure and no Medium or High Sensitivity data shall be transmitted, received, or displayed. When Medium or High data needs to be transmitted, received, or displayed, users shall use CFPB-hosted tools to conduct the teleconferences/virtual meetings with external parties, or CFPB users may use a U.S. Federal Agency's platform that has been approved through FedRAMP at a Moderate level or above, as confirmed by Cybersecurity. If the FedRAMP status is unknown or unconfirmed, then the channel should be treated as insecure until confirmed.

2. Information Sharing in Teleconferences/Virtual Meetings with External Parties
   CFPB users shall not disclose Medium or High Sensitivity information regardless of information classification. This includes sharing information orally, on a display, via screen share, attaching documents, through meeting requests/calendar invites, or any other form of information sharing.

3. Screen Sharing
   CFPB users shall not share desktop(s), transfer user control, or view/modify data with external users on third-party originated teleconferences/virtual meetings outside the Bureau firewall whom have not obtained proper Bureau-user background adjudication or credentials in compliance with federal and Bureau security and privacy requirements.

[4] For more details on Controlled Unclassified Information, see Executive Order 13556 available at http://www.whitehouse.gov/thepress-office/2010/11/04/executive-order-controlled-unclassified-information

(b) (5)

For additional information on Cybersecurity, including policies, processes, standards, and templates, visit (b) (6)

V. Legal Authorities and References

1. *Federal Information Security Modernization Act of 2014* (FISMA), PL 113-283, 128 Stat. 3073 (2014) (codified at 44 U.S.C. § 3551 *etseq.*
2. Privacy Act of 1974, 5 U.S.C. § 552a, as amended.
3. Office of Management and Budget 19-21 *Transition to ElectronicRecords*
4. Office of Management and Budget A-130 *Managing Information as a StrategicResource*

   NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations Paperwork Reduction Act of 1995* U.S.C. § 552a, as amended

VI. Revision History

(b) (5)

[redacted]

VII. Signatures and Date

Directive Owner

(b) (6)

[redacted] Digitally signed by Donna Roy
Date: 2020.04.20
16:54:20 -04'00' ________ (Signature and Date)

Donna Roy
Chief Information Officer

Approving Authority

(b) (6)

[redacted] 4/21/2020
______________ (Signature and Date)

Kate Fulton
Chief Operating Officer

VIII. Effective and Expiration Dates

The directive shall be effective as of the date of its approval or upon such other date that it specifies; and (2) the directive shall continue in effect until the COO revises or rescinds it or until such other date is specified.

Audit Report
2019-IT-C-015
October 31, 2019

Bureau of Consumer Financial Protection

2019 Audit of the Bureau's Information Security Program

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Executive Summary, 2019-IT-C-015, October 31, 2019

2019 Audit of the Bureau's Information Security Program

Findings

Since our review last year, the Bureau of Consumer Financial Protection (Bureau) has matured its information security program. Specifically, we found that the Bureau's information security program is operating effectively at a level-4 (*managed and measurable*) maturity. For instance, the Bureau's information security continuous monitoring process is effective, with the agency enhancing the functionality of its security information and event-monitoring tool. Further, the Bureau's incident response process is similarly effective, with the agency using multiple tools to detect and analyze incidents and track performance metrics.

We identified opportunities for the Bureau to strengthen its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five Cybersecurity Framework security functions—*identify, protect, detect, respond,* and *recover*—to ensure that its program remains effective. Specifically, as we noted last year, the agency can strengthen its enterprise risk management program by defining a risk appetite statement and associated risk tolerance levels. Further, the Bureau has not identified its high-value assets and determined what governance and security program changes may be needed to effectively manage security for those assets. Additionally, we identified improvements needed in the implementation of the Bureau's security assessment and authorization processes to manage security risks prior to deploying Bureau systems. We also identified improvements needed in database security, timely remediation of vulnerabilities, and patching of mobile phone operating systems.

Finally, the Bureau has taken sufficient action to close 3 of the 10 recommendations from our prior FISMA audits that remained open at the start of this audit. The closed recommendations relate to data protection and privacy, incident response, and contingency planning. We are leaving open 7 recommendations in the areas of risk management, configuration management, and identity and access management. We will continue to monitor the Bureau's progress in these areas as part of future FISMA reviews.

Recommendations

This report includes 7 new recommendations designed to strengthen the Bureau's information security program in the areas of risk management, identity and access management, data protection and privacy, incident response, and contingency planning. In its response to a draft of our report, the Bureau concurs with our recommendations and outlines actions that have been or will be taken to address them. We will continue to monitor the Bureau's progress in addressing these recommendations as part of future audits.

Purpose

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Bureau. Our specific audit objectives, based on the legislation's requirements, were to evaluate the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

Background

FISMA requires each Inspector General to conduct an annual independent evaluation of its agency's information security program, practices, and controls for select systems. U.S. Department of Homeland Security guidance for FISMA reporting directs Inspectors General to evaluate the maturity level (from a low of 1 to a high of 5) of their agencies' information security programs across several areas. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security.

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Recommendations, 2019-IT-C-015, October 31, 2019

2019 Audit of the Bureau's Information Security Program

Number	Recommendation	Responsible office
1	Determine which components of an HVA program are applicable to the Bureau and ensure the implementation of a governance structure and HVA-specific baselines and planning activities, as appropriate.	Office of the Chief Operating Officer, Office of the Chief Data Officer, and Office of Technology and Innovation
2	Ensure that established SA&A processes are performed prior to the deployment of all cloud systems used by the Bureau.	Office of Technology and Innovation
3	Ensure that user-access agreements are consistently utilized to approve and maintain access to Bureau systems for nonprivileged users.	Office of Technology and Innovation
4	Conduct a comprehensive, risk-based review to determine the optimal resources and process for prioritizing the review and adjudication of background investigations.	Office of Administrative Operations
5	Perform a risk assessment to determine a. the optimal deployment of the Bureau's technology for monitoring and controlling data exfiltration to all network access points. b. appropriate access to internet storage sites.	Office of Technology and Innovation
6	Ensure that data captured in security and privacy incident processes and tickets are accurate, consistent, and of high quality.	Office of Technology and Innovation and Office of the Chief Data Officer
7	Ensure that system-level BIAs are conducted, as appropriate, and that the results are incorporated into contingency planning strategies and processes.	Office of Technology and Innovation

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

MEMORANDUM

DATE: October 31, 2019

TO: Distribution List

FROM: Peter Sheridan Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2019-IT-C-015: *2019 Audit of the Bureau's Information Security Program*

We have completed our report on the subject audit. We performed this audit pursuant to requirements in the Federal Information Security Modernization Act of 2014 (FISMA), which requires each agency Inspector General to conduct an annual independent evaluation of the effectiveness of their agency's information security program and practices. As part of our work, we analyzed key FISMA-related data and conducted technical testing; the detailed results of that testing will be transmitted under a separate, restricted cover. In addition, we will use the results of this audit to respond to specific questions in the U.S. Department of Homeland Security's *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

We provided you with a draft of our report for review and comment. In your response, you concur with our recommendations and outline actions that have been or will be taken to address our recommendations. We have included your response as appendix B to our report.

We appreciate the cooperation that we received from Bureau personnel during our review. Please contact me if you would like to discuss this report or any related issues.

cc: Tiina Rodrigue
Tannaz Haddadi
Marianne Roth
Kirsten Sutton
Elizabeth Reilly
Dana James
Lauren Hassouni
Carlos Villa

Distribution:
Katherine Sickbert, Acting Chief Information Officer
Kate Fulton, Chief Operating Officer

Martin Michalosky, Chief Administrative Officer
Ren Essene, Chief Data Officer

Contents

Introduction

Objectives

Our audit objectives, based on the requirements of the Federal Information Security Modernization Act of 2014 (FISMA), were to evaluate the effectiveness of the Bureau of Consumer Financial Protection's (Bureau) (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. Our scope and methodology are detailed in appendix A.

Background

FISMA requires agencies to develop, document, and implement an agencywide security program for the information and the information systems that support the operations and assets of the agency, including those provided by another agency, a contractor, or another source.[1] FISMA also requires that each Inspector General (IG) perform an annual independent evaluation to determine the effectiveness of the information security program and practices of its respective agency, including testing the effectiveness of information security policies, procedures, and practices for select systems.

To support independent evaluation requirements, the U.S. Department of Homeland Security (DHS) publishes FISMA reporting metrics for IGs to respond to on an annual basis. The *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* directs IGs to evaluate the effectiveness of agency information security programs across a variety of attributes grouped into eight security domains.[2] These domains align with the five security functions defined by the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (table 1).[3]

[1] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014) (codified at 44 U.S.C. §§ 3551–3558).

[2] U.S. Department of Homeland Security, *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,* Version 1.3, April 9, 2019.

[3] The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise.

Table 1. Cybersecurity Framework Security Functions, Objectives, and Associated FISMA IG Reporting Domains

Security function	Security function objective	Associated FISMA IG reporting domain
Identify	Develop an organizational understanding to manage cybersecurity risk to agency assets	Risk management
Protect	Implement safeguards to ensure delivery of critical infrastructure services as well as prevent, limit, or contain the impact of a cybersecurity event	Configuration management, identity and access management, data protection and privacy, and security training
Detect	Implement activities to identify the occurrence of cybersecurity events	Information security continuous monitoring
Respond	Implement processes to take action regarding a detected cybersecurity event	Incident response
Recover	Implement plans for resilience to restore any capabilities impaired by a cybersecurity event	Contingency planning

Source. U.S. Department of Homeland Security, *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

As noted in DHS's IG FISMA reporting metrics, one of the goals of the annual IG FISMA evaluation is to assess agencies' progress toward achieving outcomes that strengthen federal cybersecurity, including implementation of the administration's priorities. Two of these priorities are agency progress in implementing high-value asset (HVA) programs and supply chain management security best practices. Specifically, Office of Management and Budget (OMB) Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, requires all federal agencies to establish an HVA governance structure and take a strategic, enterprisewide view of cyber risks to HVAs.[4] Additionally, the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act of 2018 (SECURE Technology Act) was passed to, in part, strengthen federal acquisition supply chain security.[5] As such, the IG FISMA reporting metrics have been updated to gauge the effectiveness of an agency's HVA program as well as its preparedness for addressing the SECURE Technology Act, while recognizing that specific guidance on supply chain risk management will be issued later.

[4] OMB Memorandum M-19-03 notes that agencies may designate federal information or information systems as HVAs when (1) the information or information system that processes or stores the information is of high value, (2) the agency that owns the HVA cannot accomplish its primary mission-essential function within expected time frames without the information or information system, or (3) the information or information system serves a critical function in maintaining the security and resilience of the federal enterprise.

[5] Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act, Pub. L. No. 115-390, 128 Stat. 3073 (2018) (codified at 44 U.S.C. §§ 3553–3554).

FISMA Maturity Model

FISMA requires that IGs assess the effectiveness of information security controls that support the operations and assets of their respective agency. To that end, the Council of the Inspectors General on Integrity and Efficiency, in coordination with OMB, DHS, and other key stakeholders, developed a maturity model intended to better address and report on the effectiveness of an agency's information security program. The purpose of the maturity model is to (1) summarize the status of agencies' information security programs and their maturity on a five-level scale; (2) provide transparency to agency Chief Information Officers (CIOs), top management officials, and other interested readers of IG FISMA reports regarding what has been accomplished and what still needs to be implemented to improve the information security program; and (3) help ensure that annual FISMA reviews are consistent across IGs.

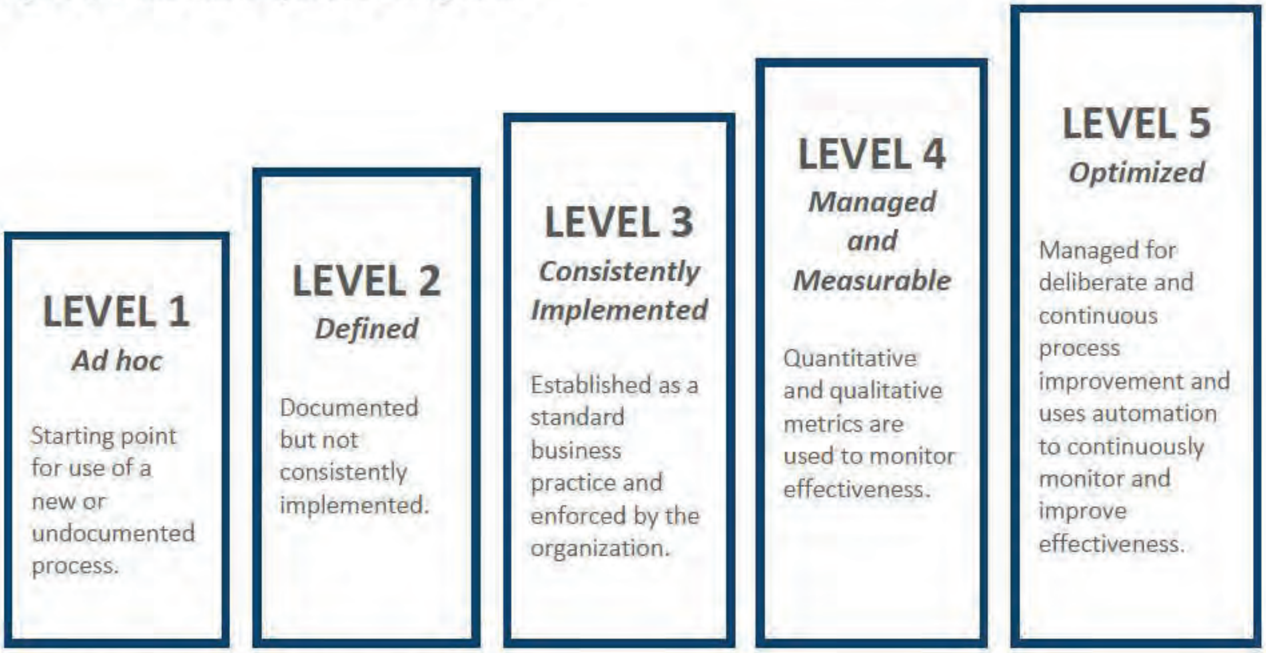
The five levels of the IG FISMA maturity model are

1. *ad hoc*
2. *defined*
3. *consistently implemented*
4. *managed and measurable*
5. *optimized*

The foundational levels (1–3) of the model are geared toward the development and implementation of policies and procedures, and the advanced levels (4–5) capture the extent to which agencies institutionalize those policies and procedures (figure 1). The maturity levels of each of the security domains will dictate the overall maturity of an organization's information security program. As noted in the IG FISMA reporting metrics, level 4 (*managed and measurable*) represents an effective level of security.[6] This is the third year that all FISMA security domains will be assessed using a maturity model. Details on the scoring methodology for the maturity model can be found in appendix A.

[6] NIST Special Publication 800-53, Revision 4, *Security and Privacy of Controls for Federal Information Systems and Organizations*, defines security control effectiveness as the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment or enforcing or mediating established security policies.

Figure 1. FISMA Maturity Model Rating Scale



LEVEL 1
Ad hoc

Starting point for use of a new or undocumented process.

LEVEL 2
Defined

Documented but not consistently implemented.

LEVEL 3
Consistently Implemented

Established as a standard business practice and enforced by the organization.

LEVEL 4
Managed and Measurable

Quantitative and qualitative metrics are used to monitor effectiveness.

LEVEL 5
Optimized

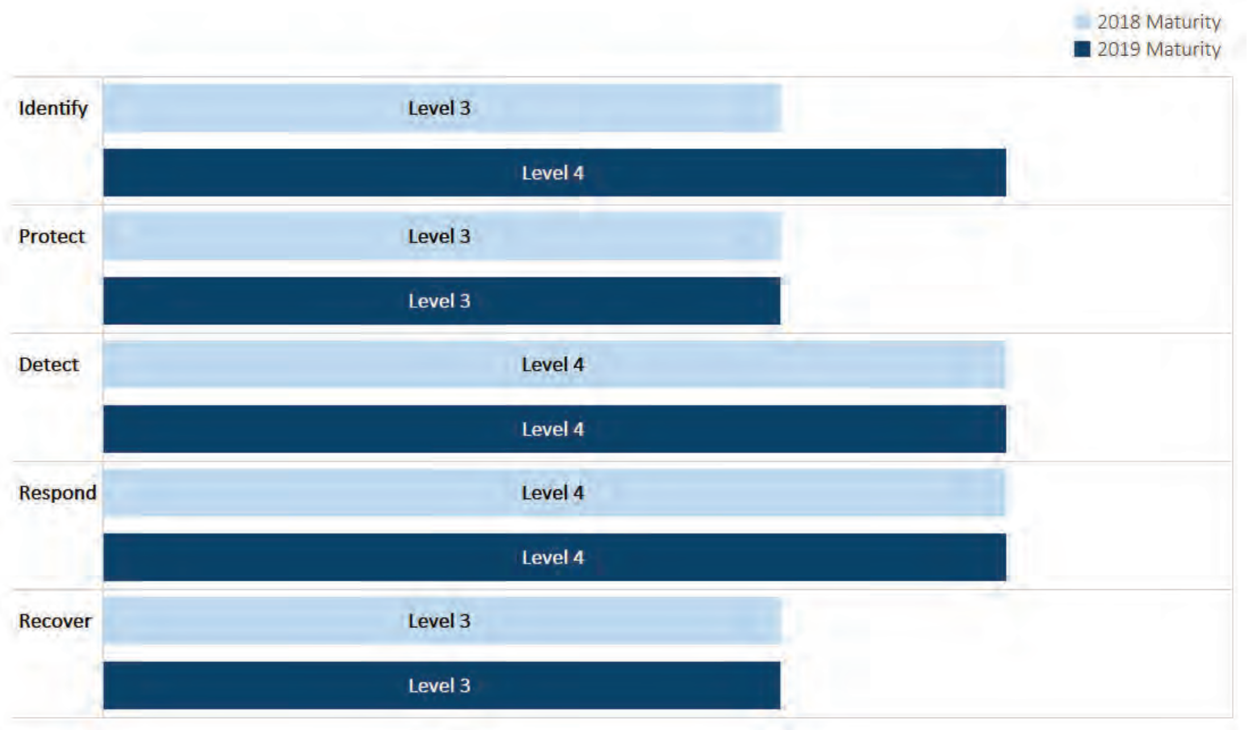
Managed for deliberate and continuous process improvement and uses automation to continuously monitor and improve effectiveness.

Source. OIG analysis of DHS IG FISMA reporting metrics.

Analysis of the Bureau's Progress in Implementing Key FISMA Information Security Program Requirements

The Bureau's overall information security program is operating effectively at a level-4 (*managed and measurable*) maturity (figure 2).[7] For instance, within the *identify* function, the Bureau strengthened its hardware asset management program by employing automation to track the life cycle of its hardware assets. Although the agency has strengthened its information security program since our 2018 FISMA review, it has further opportunities to ensure that the program is effective across specific FISMA domains in all five NIST Cybersecurity Framework security functions: *identify, protect, detect, respond,* and *recover*. Our report includes 7 recommendations in these areas as well as several items for management's consideration.

Figure 2. Maturity of the Bureau's Information Security Program



Source. OIG analysis.

[7] To determine the maturity of the Bureau's information security program, we used the scoring methodology outlined in the IG FISMA reporting metrics. Appendix A provides additional details on the scoring methodology.

Identify

The objective of the *identify* function in the Cybersecurity Framework is to develop an organizational understanding of how to manage cybersecurity risks to agency systems, assets, data, and capabilities. The Cybersecurity Framework highlights risk management processes that organizations can implement to inform and prioritize decisions. Examples of the areas in this security function, as outlined in the IG FISMA reporting metrics, that we assessed include the Bureau's processes for enterprise risk management (ERM), securing HVAs, developing and implementing an enterprise architecture, asset management, and using plans of action and milestones to manage the remediation of security weaknesses.

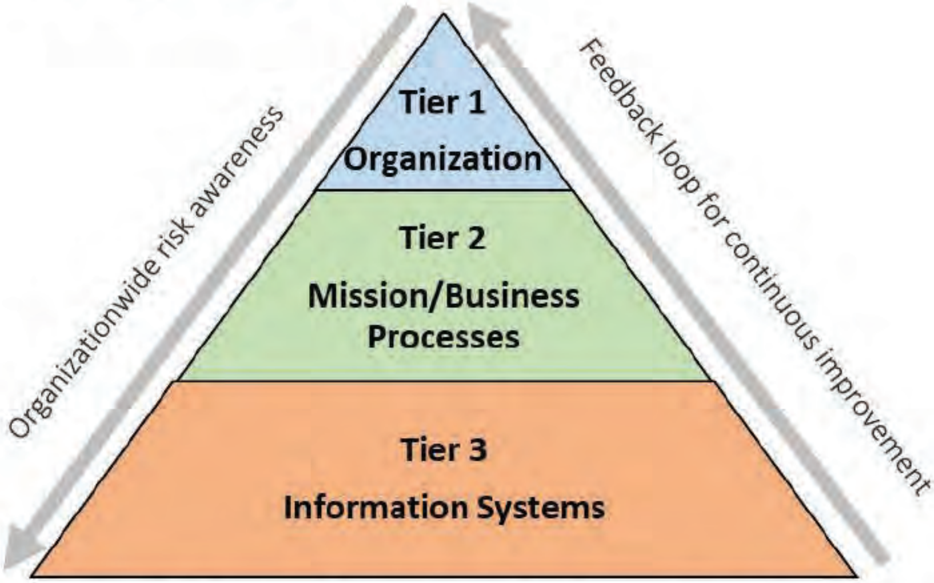
Risk Management

FISMA requires federal agencies to provide information security protections commensurate with their risk environment and to ensure that information security management processes are integrated with strategic, operational, and budgetary planning processes. Risk management refers to the program and supporting processes used to manage risk to organizational operations, assets, and individuals and is a holistic activity that affects every aspect of the organization. Risk management is further emphasized in OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, which states that an effective ERM program promotes a common understanding for recognizing and describing potential risks that can affect an agency's mission. Such risks can include cybersecurity,[8] strategic, market, legal, and reputational.

The relationships between cybersecurity risk management and ERM are further outlined in NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* (SP 800-39), which notes that effective risk management involves integration of activities at the enterprise, mission and business process, and information system levels. As depicted in figure 3, the risk management process is to be carried out across these three tiers with the overall objective of continuous improvement in the organization's risk-related activities and effective communication among all stakeholders having a shared interest in the success of the organization.

[8] According to Executive Order, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, cybersecurity risk management refers to the full range of activities undertaken to protect information technology and data from unauthorized access and other cyber threats, to maintain awareness of cyber threats, to detect anomalies and incidents adversely affecting IT and data, and to mitigate the impact of, respond to, and recover from incidents.

Figure 3. The Three Tiers of Risk Management


Tier 1
Organization
Tier 2
Mission/Business Processes
Tier 3
Information Systems
Organizationwide risk awareness
Feedback loop for continuous improvement

Source. NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View.*

Tier 1 addresses risk from an organizational perspective, providing the context for risk management activities carried out by the organization at tiers 2 and 3. NIST SP 800-39 notes that at tier 1, organizations are required to frame risk, which involves establishing the overall context for risk-based decisions. This context is established through the development of an ERM program. ERM refers to an effective agencywide approach to addressing the full spectrum of the agency's external and internal risks and includes the establishment of an organizationwide risk management strategy. Examples of ERM activities include the establishment of an enterprisewide risk management strategy and a supporting governance structure that includes the designation of a risk executive function. Additionally, ERM activities include the definition of the organization's risk appetite, risk tolerance, and risk profile.[9]

NIST SP 800-39 also notes that a key output of tier 1 risk management activities is the prioritization of mission and business functions. Specifically, more-critical mission and business functions necessitate a greater degree of risk management investments than those functions that are deemed less critical. NIST SP 800-39 further states that the determination of the relative importance of the mission and business functions, and hence the level of risk management investment, is decided at tier 1, executed at tier 2, and influences risk management activities at tier 3.

Tier 2 addresses risk from the mission and business process perspective and is informed by the risk context, decisions, and activities at tier 1. Risk management activities at tier 2 include prioritizing mission and business processes and defining the types and criticality of information needed to successfully execute the mission and business processes. These activities, along with the prioritization of mission and

[9] OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, provides guidance for implementing an ERM capability and governance structure that is coordinated with strategic planning and internal control processes.

business functions at tier 1, can serve as a key input into the development of an HVA program. OMB Memorandum M-19-03 requires agencies to take a strategic, enterprisewide view of cyber risk and bolster protections of their HVAs to improve risk management across the government.[10] HVAs are information and information systems that are deemed the most critical and high impact to agency and federal government operations.

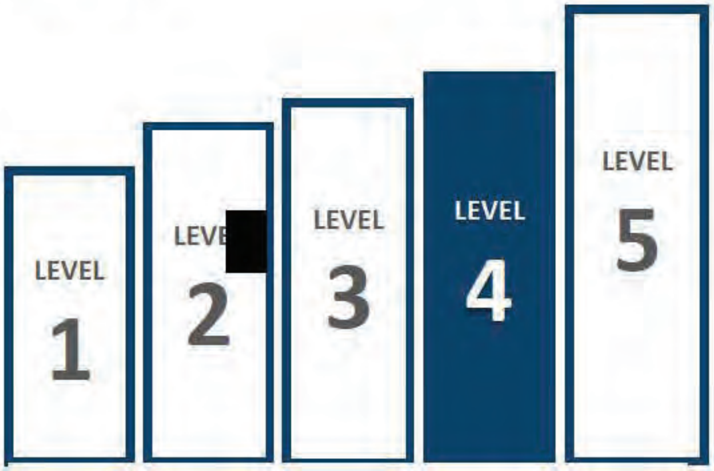
Another key tier 2 activity, as noted in SP 800-39, is the incorporation of information security requirements into mission and business processes, resulting in the development of an enterprise architecture. An enterprise architecture provides a disciplined and structured approach to achieving consolidation, standardization, and optimization of information technology (IT) assets that are employed within organizations. The information security architecture, which is a component of the enterprise architecture, influences and guides the allocation of information protections needs, which affects the allocation of specific security controls at tier 3.

Tier 3 addresses risk from an information system perspective and is guided by the risk context, risk decisions, and risk activities at tiers 1 and 2. Tier 3 risk management activities include the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls for all of the organization's information systems. NIST SP 800-39 notes that the risk management activities at tier 3 reflect the organization's risk management strategy and any risk related to the cost, schedule, and performance requirements for individual information systems supporting the mission and business functions of organizations. Such requirements include specific control considerations for an organization's HVAs.

Current Security Posture

We found that the Bureau has matured its risk management program from a level-3 maturity in 2018 to a level-4 (*managed and measurable*) maturity, which represents an effective level of maturity (figure 4). For instance, the Bureau employs automation to track the life cycle of its hardware assets. Further, the Bureau maintains qualitative and quantitative performance measures related to its plans of action and milestones process.

Figure 4. Risk Management, Level 4 (*Managed and Measurable*)



Source. OIG analysis.

We have made several recommendations in prior FISMA reports for strengthening the Bureau's risk management program, including in the areas of insider threat and ERM. Our 2016 FISMA audit report included a recommendation for the CIO to

[10] In November 2017, DHS published the *High Value Asset Control Overlay* to provide technical guidance to federal civilian agencies on securing HVAs.

evaluate options and develop an agencywide insider threat program that includes (1) a strategy to raise organizational awareness; (2) an optimal organizational structure; and (3) integration of incident response capabilities, such as ongoing activities around data loss prevention.[11] This year, the Bureau developed an *Insider Threat Program Communications Plan* that defines various components of an insider threat program, including communication channels and roles and responsibilities. However, we found that the Bureau has not fully implemented its data loss prevention tool across the enterprise. As such, we are leaving our 2016 recommendation open and will continue to monitor the Bureau's efforts in this area as part of our future FISMA reviews.

In addition, in our 2017 FISMA audit report, we recommended that the Chief Risk Officer continue to work with divisions across the Bureau to ensure that a risk appetite statement and associated risk tolerance levels are defined and used to develop and maintain an agencywide risk profile.[12] This year, we found that the Bureau has updated its risk profile and conducted an agencywide security and privacy risk assessment. However, the Bureau has not approved a risk appetite statement and finalized tolerance levels. As such, we are leaving this recommendation open and will continue to monitor the Bureau's efforts in this area as part of our future FISMA reviews.

Opportunities for Improvement

We identified several opportunities to strengthen the agency's risk management program at the organization level (tier 1), mission and business process level (tier 2), and information system level (tier 3). We believe that strengthening these areas will allow the Bureau to improve its risk management program.

Organization Level (Tier 1)

One key output of tier 1 is the development of an ERM program to address the full spectrum of the agency's risks and provide the overall context in which risk management decisions are made across the organization. As noted above, the Bureau is still working to define its risk appetite statement and tolerance levels as part of its ERM implementation. Completion of the risk appetite statement and tolerance levels will affect risk-based decisionmaking at other tiers. Further, we noted that the Office of Technology and Innovation is using an automated tool to track system-level risk management activities. However, from an organizationwide perspective, the Bureau has not determined how it will use technology, such as a governance, risk management, and compliance tool, at the organizational level to provide a centralized, enterprisewide view of risks. As mentioned in our 2017 and 2018 FISMA reports, we realize that the implementation of such technologies depends on the Bureau fully implementing its ERM management strategy and related components. Further, such tools are offered through DHS's Continuous Diagnostics and Mitigation (CDM) program. As further detailed in the information security continuous monitoring (ISCM) section of our report, the Bureau is working with DHS to determine which components of the CDM program it will implement. As part of this effort, we believe that the Bureau should determine whether there are tools offered through CDM that will meet the agency's needs in this area. Because the Bureau's CDM implementation is in progress, we are not making a recommendation in

[11] Office of Inspector General, *2016 Audit of the CFPB's Information Security Program,* OIG Report 2016-IT-C-012, November 10, 2016.

[12] Office of Inspector General, *2017 Audit of the CFPB's Information Security Program,* OIG Report 2017-IT-C-019, October 31, 2017.

this area. We will continue to monitor the Bureau's efforts to use technology to strengthen its ERM program.

Mission and Business Process Level (Tier 2)

As noted earlier, a key activity in tier 2 is developing and implementing an HVA program for the information and information systems that are deemed the most critical and high impact to agency and federal government operations. Specifically, OMB Memorandum 19-03 requires agencies to take a number of steps to protect their HVAs against evolving cyber threats. These steps are outlined in table 2 and collectively represent the components of an HVA program.

Table 2. Key HVA Program Requirements

Requirement	Description
Establish enterprise HVA governance	Designate an HVA governance structure to incorporate HVA activities into broader agency activities, such as ERM, contracting processes, and contingency planning.
Improve the designation of HVAs	Identify and designate federal information or a federal information system as an HVA based on information value, support of mission-essential functions, and support of a critical function in maintaining the security and resilience of the federal civilian enterprise.
Implement data-driven prioritization	Allocate appropriate resources and ensure the effective protection of HVAs through collaboration and data-driven prioritization.
Increase the trustworthiness of HVAs	Implement systems security engineering principles for all HVAs to include security and privacy requirements.
Protect the privacy of HVAs	Ensure that privacy documentation and materials are maintained for HVAs that create, process, use, store, maintain, disseminate, disclose, or dispose of personally identifiable information.

Source. OIG analysis of OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, December 10, 2018.

The Bureau has not established a formal HVA program and properly identified its HVAs, in accordance with federal guidance. Specifically, the Bureau initially classified all of its information systems as HVAs. We did not find evidence, however, that the Bureau arrived at this determination by using DHS and OMB guidance or by performing a formal assessment to identify its HVAs. Office of Technology and Innovation officials stated that they are in the process of performing a comprehensive assessment to determine the agency's HVAs and anticipate completing this effort by the end of the third quarter of 2019. We believe that by properly identifying its HVAs and establishing an overall HVA program, as appropriate, the Bureau will have greater assurance that its key systems and data are adequately protected.

Information Systems Level (Tier 3)

A key step in tier 3 is the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls for all of the organization's information systems, including HVAs. With respect to HVAs, OMB Memorandum M-19-03 requires that agencies implement the system security engineering principles outlined in NIST Special Publication 800-160, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems,* and ensure that security and privacy requirements for all HVAs reflect these principles. In addition, DHS has issued guidance that provides additional specifications for protections applied to HVAs.[13] This guidance notes that the additional HVA control specifications are intended to be applied after an agency has selected and applied either the high or moderate security baselines for all information systems specified by NIST. We found that while the Bureau has developed control baselines for its information systems in accordance with NIST guidance, the agency has not defined additional security controls and enhancements that will apply to its HVAs. We believe that as the Bureau defines its HVA program, it should ensure that any additional security controls and enhancements beyond those that apply to all Bureau systems are identified, defined, and communicated.

Further, we identified improvements needed in the implementation of the Bureau's security assessment and authorization (SA&A) process. Specifically, we found that the agency deployed two of three cloud-based systems that we sampled without completing a comprehensive system security plan, conducting an agency-specific risk and security controls assessment, or granting an authorization to operate (ATO). Bureau officials attributed this issue to an overreliance on vendors and internal oversight. Further, once we notified the Bureau of these issues, agency officials took immediate steps to ensure that SA&A activities were initiated. As a result of these weaknesses, there is increased risk that cloud-based systems in use do not meet the Bureau's information security requirements. For example, as noted in the identity and access management section of our report, we found weaknesses in the Bureau's management of user-access forms for one of the cloud-based systems that had not gone through the agency's SA&A process. We believe that this issue may have been flagged if the Bureau's SA&A process had been followed prior to system deployment.

The Bureau's *Information Security Program Policy* notes that the agency uses the foundational process of SA&A to document and manage the security posture of new and existing systems, including cloud systems, and their operating environments. Table 3 outlines key components of the Bureau's SA&A processes as they relate to system security planning, risk and security controls assessment, and ATO.

[13] U.S. Department of Homeland Security, *High Value Asset Control Overlay*, Version 1.0, November 2017.

Table 3. Key Activities Supporting the Bureau's SA&A Process

Activity	Requirement and description
System security planning	The system security plan specifies the security requirements applicable to the system and the protection mechanisms implemented to meet those requirements. System owners are required to develop a system security plan for each major information system.
Risk and security control assessment	The Bureau has developed a formalized process to assess the risks associated with the operation of agency information systems. As part of this process, a security controls assessment is required to determine whether selected security controls are implemented correctly, operate as intended, and are effective in achieving security objectives. The mitigation of weaknesses that are discovered through this process is managed through a plan of action and milestones.
ATO	An ATO is 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. All new Bureau systems, including cloud systems, are required to be granted an ATO prior to being operated in a production environment.

Source. OIG analysis of the Bureau's information security program and risk management process.

In our 2019 report, *The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP*, we identified a similar issue with respect to a cloud system approved by the Federal Risk and Authorization Management Program (FedRAMP) and used by the Bureau.[14] Specifically, we found that the Bureau did not ensure that its SA&A process was followed for a FedRAMP-approved cloud system used by the agency to support its call center operations prior to its deployment.[15] We recommended that the CIO ensure that established SA&A processes are (1) performed prior to the deployment of all FedRAMP-approved cloud systems used by the Bureau and (2) used to make an agency-specific authorization decision for the system that is in production and noted in our report. The issues we identified in the current report are for Bureau-used cloud systems that are *not* provided through FedRAMP, and, as such, we are making a recommendation for the Bureau to strengthen its SA&A processes for all cloud systems. We believe that by ensuring that SA&A activities are completed prior to onboarding cloud systems, the Bureau will have greater assurance that controls are effectively implemented to protect sensitive agency information.

[14] FedRAMP was established in December 2011. One of the goals of FedRAMP is to provide a cost-effective, risk-based approach to the adoption and use of cloud service by federal agencies. The Bureau uses several FedRAMP-approved cloud systems.

[15] Office of Inspector General, *The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP*, OIG Report 2019-IT-C-009, July 17, 2019.

Recommendations

We recommend that the Chief Operating Officer, the Chief Data Officer, and the CIO

1. Determine which components of an HVA program are applicable to the Bureau and ensure the implementation of a governance structure and HVA-specific baselines and planning activities, as appropriate.

We recommend that the CIO

2. Ensure that established SA&A processes are performed prior to the deployment of all cloud systems used by the Bureau.

Management Response

The Acting CIO concurs with these recommendations. The Acting CIO notes that the Bureau will review how an HVA program may apply to the agency to ensure that resulting governance processes incorporate related activities, such as identification of HVA and applicable controls or processes, into ERM. Further, the Acting CIO notes that, moving forward, all Bureau systems will undergo the SA&A processes before being deployed for production use.

OIG Comment

We believe that the actions described by the Bureau are responsive to our recommendations. We plan to follow up on the Bureau's actions to ensure that the recommendations are fully addressed.

Protect

The objective of the *protect* function in the Cybersecurity Framework is to develop and implement safeguards to secure information systems. This function supports the ability to prevent, limit, or contain the impact of a cybersecurity event through applicable configuration management, identity and access management, data protection and privacy, and security training processes. Table 4 summarizes the security domains that are included in this security function and the associated assessment areas, as outlined in the IG FISMA reporting metrics, that we assessed.

Table 4. *Protect* Function Security Domains and Selected Components

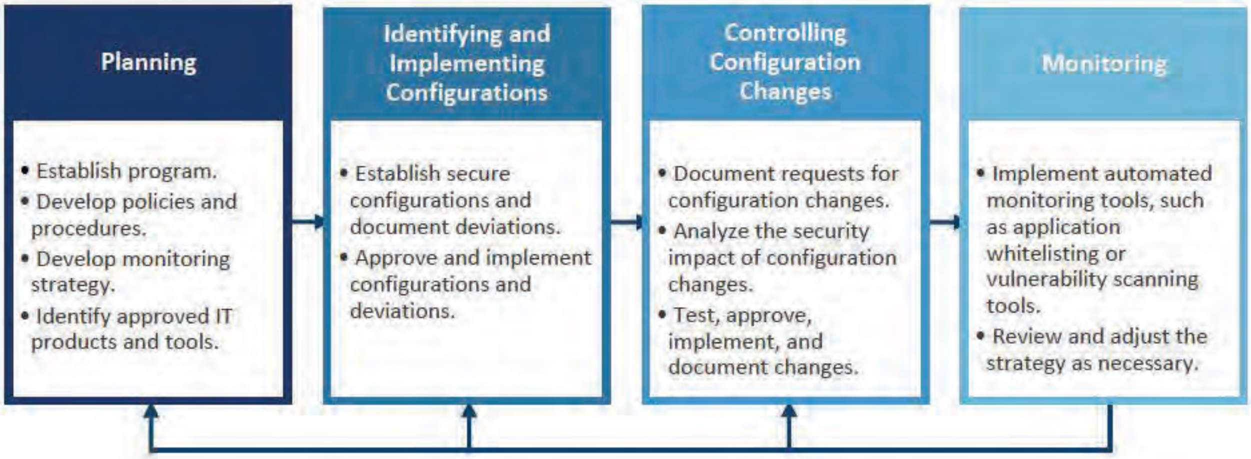
Security domains	Examples of components assessed by IGs
Configuration management	Configuration management plans, configuration settings, flaw remediation, and change control
Identity and access management	Identity credential and access management strategy, access agreements, and background investigations
Data protection and privacy	Security controls for exfiltration, privacy security controls, and privacy awareness training
Security training	Assessment of knowledge, skills, and abilities; security awareness; and specialized security training

Source. U.S. Department of Homeland Security, *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

Configuration Management

FISMA requires agencies to develop an information security program that includes policies and procedures that ensure compliance with minimally acceptable system configuration requirements. Configuration management refers to a collection of activities focused on establishing and maintaining the integrity of products and information systems through the control of processes for initializing, changing, and monitoring their configurations. NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, recommends integrating information security into configuration management processes. Security-focused configuration management of information systems involves a set of activities that can be organized into four major phases: (1) planning, (2) identifying and implementing configurations, (3) controlling configuration changes, and (4) monitoring (figure 5).

Figure 5. Security-Focused Configuration Management Phases


Planning
• Establish program.
• Develop policies and procedures.
• Develop monitoring strategy.
• Identify approved IT products and tools.
Identifying and Implementing Configurations
• Establish secure configurations and document deviations.
• Approve and implement configurations and deviations.
Controlling Configuration Changes
• Document requests for configuration changes.
• Analyze the security impact of configuration changes.
• Test, approve, implement, and document changes.
Monitoring
• Implement automated monitoring tools, such as application whitelisting or vulnerability scanning tools.
• Review and adjust the strategy as necessary.

Source. NIST Special Publication 800-128, *Guide for Security-Focused Configuration Management of Information Systems*.

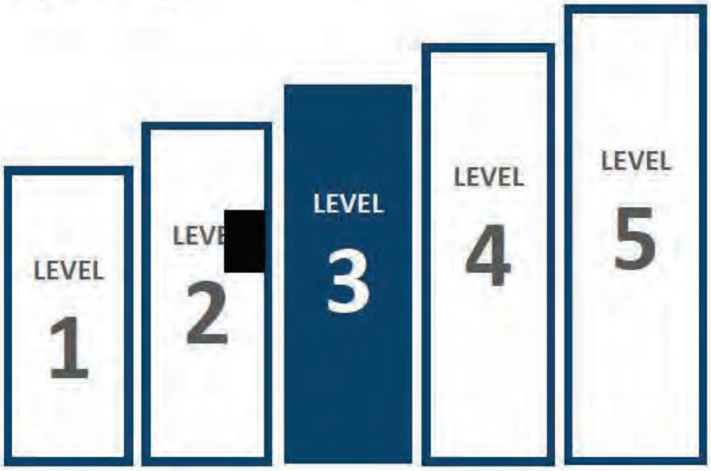
A key component of security-focused configuration management is monitoring, which involves validating that information systems are adhering to organizational policies, procedures, and approved secure configuration baselines. When inconsistencies are identified, the organization should take action to mitigate resulting security risks. Monitoring processes are also needed to identify software security updates and patches that need to be installed for an organization's technology environment. Unpatched or outdated software can expose an organization to increased risk of a cyberattack.

With respect to patch management, NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (SP 800-53), notes that organizations should install security-relevant software and firmware updates within organization-defined time frames and incorporate flaw remediation into configuration management processes. In addition, NIST Special Publication 800-40, Revision 3, *Guide to Enterprise Patch Management Technologies*, states that for products and systems, including mobile devices, applying patches corrects security and functionality problems in software and firmware and reduces opportunities for exploitation. It also states that the use of an enterprise mobile device management software is an option to keep mobile device software updated and can restrict access if the device's operating system is not up to date.

Current Security Posture

The Bureau's configuration management program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level (figure 6). For instance, the Bureau employs network access controls to detect unauthorized hardware. Further, the Bureau tracks and reports on performance measures related to its change control activities.

Figure 6. Configuration Management, Level 3 (*Consistently Implemented*)



Source. OIG analysis.

Opportunities for Improvement

Our previously identified issues in the areas of secure database configurations, vulnerability remediation, and mobile phone patch management continue to represent opportunities for the Bureau to mature its configuration management program. Specifically, our vulnerability scanning continues to identify weaknesses in the Bureau's database-level security configurations.[16] Similar to last year, the weaknesses identified relate to unsecure database configurations, including for controls related to audit and accountability, and system and information integrity. We initially included a recommendation to strengthen database- and application-level configuration management processes in our 2014 FISMA report.

Specifically, our 2014 FISMA report includes a recommendation for the CIO to strengthen the Bureau's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database- and application-level security configurations.[17] Last year, we found that the Bureau has implemented an application-level vulnerability-scanning tool, which the agency is using for its web applications.[18] This year, we found that the Bureau is still in the processes of identifying and implementing a database-level vulnerability scanning product. We believe that the lack of a database-level vulnerability scanning process is a key contributing cause for the database configuration weaknesses we continue to identify. Although we are not making additional recommendations in this area, we strongly suggest that the Bureau continue to prioritize the implementation of an automated solution and process to periodically assess and manage database-level security configurations. We are leaving our

[16] The Bureau provided us with authorized access to its network and administrative credentials to perform scanning within its internal network. The detailed results of our follow-up work in this area will be transmitted to the Bureau under a separate, restricted cover due to the sensitive nature of the information.

[17] Office of Inspector General, *2014 Audit of the CFPB's Information Security Program*, OIG Report 2014-IT-C-020, November 14, 2014.

[18] Office of Inspector General, *2018 Audit of the Bureau's Information Security Program*, OIG Report 2018-IT-C-018, October 31, 2018.

2014 recommendation open and will continue to follow up on the Bureau's efforts in this area as a part of future FISMA reviews.

In addition, our 2018 FISMA report includes a recommendation for the CIO to strengthen configuration management processes by (1) remediating configuration-related vulnerabilities in a timely manner and (2) ensuring that optimal resources are allocated to perform vulnerability remediation activities.[19] We continue to find that the Bureau is not timely remediating numerous critical or high-risk vulnerabilities in agency systems that it has identified through its own vulnerability scanning.[20] Further, our operating system–level vulnerability scanning identified a number of critical or high-risk vulnerabilities that had previously been identified by the Bureau's internal vulnerability scans several months earlier.[21] The Bureau's *Information Security Standards* (CS-S-01) requires that critical, high, moderate, and low vulnerabilities be remediated timely, and that for critical vulnerabilities, remediation be performed within 30 days. Bureau officials continue to note that the key cause for the delays in mitigating technical vulnerabilities is a lack of resources.

While the Bureau took steps to strengthen security controls in this area during our review, we believe that an overall process to ensure timely remediation of security vulnerabilities could better protect Bureau systems and data from compromise. As such, we are leaving our 2018 recommendation open and will monitor the Bureau's efforts in this area as part of our future FISMA reviews.

Finally, our 2018 FISMA report includes a recommendation for the CIO to develop and implement a process to ensure the timely application of patches and security updates for Bureau-issued mobile phones.[22] We continue to identify Bureau mobile devices that do not have current operating system patches applied. Bureau officials stated that by the end of 2019, the agency would update its policy to require that agency-issued mobile phones have the latest operating system and deploy a new tool to enforce the application of current patches for mobile phone operating systems. As such, we are leaving this recommendation open and will continue to follow up on the Bureau's efforts in this area as a part of future FISMA reviews.

[19] Office of Inspector General, *2018 Audit of the Bureau's Information Security Program*, OIG Report 2018-IT-C-018, October 31, 2018.

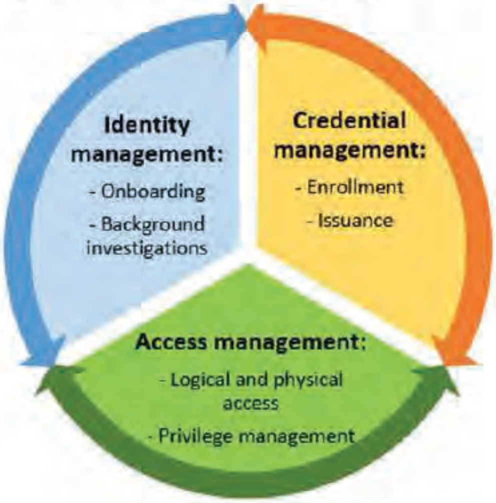
[20] While the Bureau has not implemented a database-level vulnerability scanning process or tool, the agency regularly performs vulnerability scans of its network and operating systems.

[21] The Bureau provided us with special authorized access to the network and administrative credentials to perform operating system–level scanning within its internal network.

[22] Office of Inspector General, *2018 Audit of the Bureau's Information Security Program*, OIG Report 2018-IT-C-018, October 31, 2018.

Identity and Access Management

Figure 7. ICAM Conceptual Design



Source. CIO Council, *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance.*

Identity and access management includes implementing a set of capabilities to ensure that users authenticate to IT resources and have access to only those resources that are required for their job function, a concept referred to as *need to know*. Supporting activities include onboarding and personnel screening, issuing and maintaining user credentials, and managing logical and physical access privileges, which are collectively referred to as identity, credential, and access management (ICAM) (figure 7).

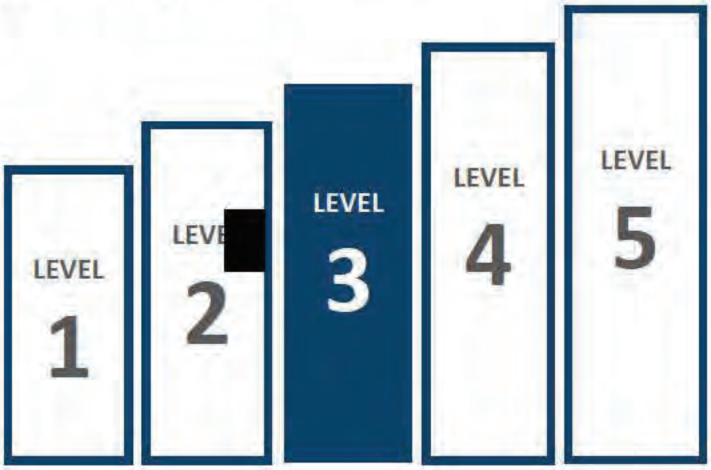
A key component of effective identity and access management is developing a comprehensive strategy that outlines the components of the agency's ICAM program within the business functions that they support. The *Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance* provides the government with a common framework and implementation guidance to plan and execute ICAM programs. Another key component of effective identity and access management is controlling the use of privileged accounts that possess elevated rights and are empowered with broad, direct access to information systems. NIST SP 800-53 emphasizes the importance of tracking and controlling access privileges and ensuring that these privileges are periodically reviewed and adjusted.

In support of federal ICAM requirements, the Bureau has developed and implemented policies and procedures that cover multiple functions throughout the life cycle of a user's digital identity. For example, the Bureau's policies and procedures cover requirements for account management, multifactor authentication, audit logging, background investigations, and onboarding. With respect to the management of privileged accounts, the Bureau's policies and procedures require privileged users to annually resubmit their signed and approved user-access forms and rules of behavior or their privileged access will be revoked.

Current Security Posture

The Bureau's identity and access management program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing certain activities indicative of a higher maturity level (figure 8). For instance, the Bureau is allocating resources to effectively implement ICAM activities and holding personnel accountable for carrying out their roles and responsibilities. The Bureau continues to consolidate ICAM investments across the agency and has defined an implementation strategy. Additionally, the Bureau has strengthened identity and access controls for its remote access program. Specifically, the Bureau is using enhanced features offered by its security information, event-monitoring, and antivirus software to perform more detailed user activity reviews for remote access sessions.

Figure 8. Identity and Access Management, Level 3 (*Consistently Implemented*)



Source. OIG analysis.

Opportunities for Improvement

Our previously identified issues in the areas of maintaining user-access agreements and rules-of-behavior forms for individuals with privileged access and requiring the use of multifactor authentication sign-on for Bureau users continue to represent opportunities for the Bureau to mature its identity and access management program. This year, we also identified improvements needed in the maintenance of user-access forms for general users and in the timely adjudication of background investigations.

In our 2018 FISMA audit report, we found that the Bureau was not consistently managing and updating its user-access agreement and rules-of-behavior documentation for a sample of privileged or administrative users. We recommended that the CIO determine whether established processes and procedures for management of user-access agreements and rules-of-behavior forms for privileged users are effective and adequately resourced and make changes as needed.[23] This year, we sampled user-access agreement and rules-of-behavior documentation for a total of 17 privileged users for the three Bureau cloud systems we sampled.[24] We found that for 14 of these privileged users, user agreement forms did not include appropriate approval of the need for access, and rules-of-behavior documents were not on file. As such, we are keeping our 2018 recommendation open and will continue to monitor the Bureau's efforts in this area as part of future FISMA reviews.

[23] Office of Inspector General, *2018 Audit of the Bureau's Information Security Program*, OIG Report 2018-IT-C-018, October 31, 2018.

[24] Per the Bureau's cybersecurity policy, a privileged user is defined as an individual who has been granted elevated privileges, which are typically allocated to system administrators, network administrators, and others who are responsible for system or application control, monitoring, or administration functions.

Further, we sampled 20 nonprivileged users for a select Bureau cloud system and found that user-access agreements were not completed for any of the users. For these users, rules-of-behavior forms were completed instead; however, these forms do not contain supervisory approval of the need for access. The Bureau's access controls policies require nonprivileged users to have authorized access to the information system based on valid access authorization and intended system usage. Further, as referenced in the risk management section of this report, this issue occurred for the same cloud system that had not gone through the Bureau's SA&A process prior to being implemented in a production environment. We believe that completion of user-access agreements prior to provisioning access to systems will provide the Bureau with greater assurance that only individuals with a business need have access to agency systems. Our report includes a new recommendation in this area.

Additionally, as we have previously reported, the Bureau has not fully implemented multifactor authentication for logical access to its information systems. In our 2017 FISMA audit report, we found that the Bureau had enabled the option for both privileged and nonprivileged users to use their personal identity verification (PIV) cards to access their computers when at the Bureau; however, it was not a requirement.[25] We recommended that the CIO develop and implement a tiered approach for implementing multifactor authentication that considers system risk levels and user roles and uses lessons learned to inform broader adoption.

This year, we found that the Bureau implemented several technical solutions that in totality did not fully meet federal requirements for multifactor authentication. Specifically, DHS guidance requires users to authenticate to an agency's network using a two-factor PIV credential or other Identity Assurance Level 3/Authenticator Assurance Level 3 credential. NIST Special Publication 800-63, *Digital Identity Guidelines,* notes that in order to authenticate at Authenticator Assurance Level 3, possession and control of two distinct factors are required. The technical solutions implemented by the Bureau did not meet these requirements. Bureau officials explained that, as they continue to move toward a cloud-only infrastructure, they plan to incorporate a hybrid approach to ICAM and are evaluating various initiatives for multifactor authentication in such an environment. As such, we are leaving our 2017 FISMA audit recommendation in this area open and will continue to follow up on the Bureau's efforts as a part of our future FISMA audits.

Finally, we found that the Bureau is not reviewing and adjudicating background investigation results received from the Office of Personnel Management (OPM) in a timely manner. Specifically, we identified 3 of a sample of 37 Bureau employees and contractors who had completed background investigations by OPM but had not received a review and adjudication by the Bureau in approximately 5 months. This included Bureau personnel with elevated access to systems with sensitive data.[26] Further, Bureau officials informed us that overall they have a backlog of approximately 300 background investigations completed by OPM for which they need to perform adjudication. Approximately 35 percent of these are for new

[25] Office of Inspector General, *2017 Audit of the CFPB's Information Security Program,* OIG Report 2017-IT-C-019, October 31, 2017.

[26] In accordance with the Bureau's personnel security policy, employees and contractors are provided access to agency systems after the completion of a fingerprint check.

employees or contractors, while the remaining 65 percent are for re-investigations of current employees and contractors.[27]

The Bureau's *Personnel Security Policy* requires that all personnel are assigned risk designations, appropriately screened prior to being granted system access, and rescreened. The adjudication and final clearance determinations are the final stage of the process to determine whether an individual is deemed eligible for access. The Bureau cited resource constraints as a contributing factor for not adjudicating completed background investigations in a timely manner. We believe that the recent lifting of the agency's hiring freeze may also affect the timely adjudication of background investigations moving forward. We believe that timely adjudication of the completed background investigations from OPM could yield additional information necessary to determine a person's eligibility to access Bureau systems. Further, timely adjudication of background investigations could help mitigate risks from insider threats.

Recommendations

We recommend that the CIO

3. Ensure that user-access agreements are consistently utilized to approve and maintain access to Bureau systems for nonprivileged users.

We recommend that the Chief Administrative Officer

4. Conduct a comprehensive, risk-based review to determine the optimal resources and process for prioritizing the review and adjudication of background investigations.

Management Response

The Acting CIO concurs with these recommendations. The Acting CIO notes that the Bureau plans to evaluate and leverage potential automated solutions to improve the tracking of all user-access requests and authorizations to Bureau systems. Further, the Acting CIO notes that the Bureau is currently undergoing an internal program review to determine the optimal allocation of resources, as well as defining a prioritization process for the review and adjudication of background investigations.

OIG Comment

We believe that the actions described by the Bureau are responsive to our recommendations. We plan to follow up on the Bureau's actions to ensure that the recommendations are fully addressed.

Data Protection and Privacy

Data protection and privacy refers to a collection of activities focused on the security objective of confidentiality, preserving authorized restrictions on information access, and disclosure to protect personal privacy and proprietary information. The need for addressing this objective is great, with agencies reporting over 31,000 security incidents to DHS in fiscal year 2018, including web-based attacks,

[27] Our audit scope did not include verification of the job functions for these individuals.

phishing attacks, and loss or theft of computing equipment.[28] In today's digital world, effectively managing the risk to individuals associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of their personally identifiable information (PII) increasingly depends on the safeguards employed for the information systems that process, store, and transmit the information. As such, OMB Circular A-130, *Managing Information as a Strategic Resource*, requires federal agencies to develop, implement, and maintain agencywide privacy programs that, where PII is involved, play a key role in information security and implementing the NIST Risk Management Framework.[29] While the head of each federal agency remains ultimately responsible for ensuring that privacy interests are protected and for managing PII responsibly within their respective agency, Executive Order 13719, *Establishment of the Federal Privacy Council*, requires agency heads to designate a senior agency official for privacy who has agencywide responsibility and accountability for the agency's privacy program.

NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (SP 800-122), notes the importance of the identification of all PII residing in the organization or under the control of a third party on behalf of the organization. Further, SP 800-122 recommends measures to protect PII and other sensitive information, including operational safeguards (for example, policies, procedures, and awareness training), privacy-specific safeguards (for example, minimizing the use, collection, and retention of PII), and security controls (for example, access control to PII, media sanitization, and the protection of data at rest or in transit).

To meet its mission of regulating the offerings and provisions of consumer financial products and services under federal consumer financial laws,[30] the Bureau collects a significant amount of sensitive PII. This information includes consumer financial data on credit card accounts, mortgage loans, arbitration case records, automotive sales, credit scores, private student loans, and storefront payday loans.

[28] U.S. Government Accountability Office, *Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices*, GAO-19-545, July 2019.

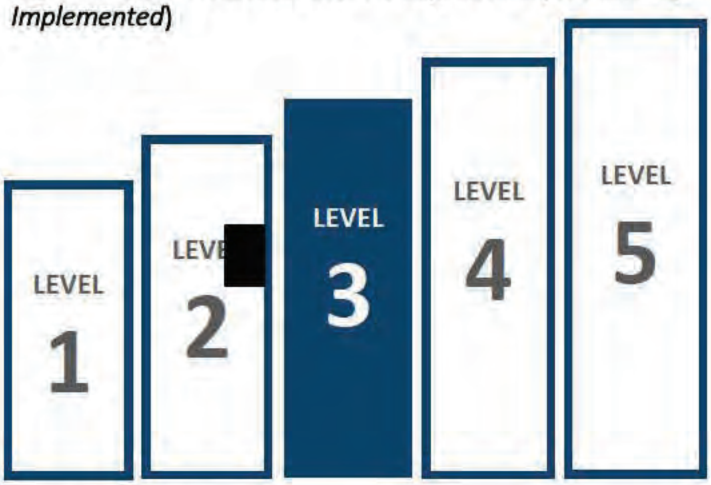
[29] NIST has developed a risk management framework to provide a structured and flexible process for managing security and privacy risk for federal information and information systems that includes security categorization, control selection, implementation and assessment, authorization, and continuous monitoring. NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*, describes the Risk Management Framework and provides guidelines for applying it to information systems and organizations.

[30] 12 U.S.C. §§ 5491(a).

Current Security Posture

The Bureau's data protection and privacy program is operating at a level-3 (*consistently implemented*) maturity, though the agency is also performing remote wiping of mobile devices, which is associated with a higher maturity level (figure 9). The Bureau has also implemented encryption for sensitive data at rest and in transit, as appropriate, and the agency restricts the use of removable storage devices.

Figure 9. Data Protection and Privacy, Level 3 (*Consistently Implemented*)



Source. OIG analysis.

In addition, the Bureau has established and maintains a privacy program to provide for the development and maintenance of privacy controls. The program includes a dedicated staff headed by a senior agency official for privacy. Further, the privacy team works with IT staff in the Office of Technology and Innovation and other stakeholders as needed for the security of sensitive data. The Bureau has also implemented annual privacy training for all staff and privacy role-based training for individuals with significant privacy-related responsibilities.

Opportunities for Improvement

Our previously identified issues in the areas of physically securing equipment and inventorying all of the agency's PII continue to represent opportunities for the Bureau to mature its data protection and privacy program. Specifically, in February 2018, we issued a report on the Bureau's privacy program that included two recommendations.[31] One recommendation related to the physical security of equipment and documents, and the other recommendation referred to an incomplete inventory of PII that the Bureau is collecting or handling, who within the Bureau is responsible for the security of the data, where it is stored, and whether a privacy impact assessment or System of Record Notice is required. During our 2018 and 2019 FISMA fieldwork, we found that the Bureau had taken steps to address both of these recommendations. For the recommendation related to the physical security of devices, we found in 2018 that the Bureau had provided new cable locks for equipment, and this year an agency official stated that the Bureau has identified further corrective actions to address the recommendation. Related to the PII inventory recommendation, this year officials informed us that they have identified the divisions that had not been reporting their PII data and that they will have a complete data catalogue in the first quarter of fiscal year 2020. While the Bureau has taken steps to address the two recommendations, all actions have

[31] Office of Inspector General, *Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program*, OIG Report 2018-IT-C-003, February 14, 2018.

not yet been completed. As such, we are leaving these two recommendations open and will continue to follow up on the Bureau's efforts as a part of future audits.[32]

Further, we identified improvements needed in the Bureau's data exfiltration controls to better ensure the protection of sensitive agency data. Specifically, we found that a technology being used by the Bureau to monitor and control data exfiltration was not consistently implemented across the Bureau's IT environment. For instance, this technology was not blocking access to known internet storage sites and was not deployed across all of the Bureau's network.[33] The Bureau's *Information Security Standards* (CS-S-01) require that the agency monitor and control communications at its external and internal system boundaries and monitor systems to detect unauthorized local, network, and remote connections. In addition, the *FY 2019 CIO FISMA Metrics* highlight the importance of checking outbound communications traffic at external boundaries to detect unauthorized exfiltration of information (for example, anomalous volumes of data, anomalous traffic patterns, elements of PII, and so on) with a solution that is centrally visible at the enterprise level.[34]

Bureau officials informed us that technical issues have prevented them from deploying their more-effective data exfiltration protections and monitoring across all areas of their environment. Further, Bureau officials stated that they have made a business decision to not block known internet storage sites because of the effect on users' experience in the environment. By ensuring that data exfiltration technologies are deployed consistently across its environment, the Bureau will have greater assurance that sensitive information is not disclosed to those who do not have a need to know.

Recommendation

We recommend that the CIO

5. Perform a risk assessment to determine
    a. the optimal deployment of the Bureau's technology for monitoring and controlling data exfiltration to all network access points.
    b. appropriate access to internet storage sites.

Management Response

The Acting CIO concurs with this recommendation and notes that the Bureau will perform a risk assessment to determine the necessary data monitoring and controlling technologies, such as data loss prevention solutions, to be deployed across applicable access points to control the flow of traffic to restricted systems and internet storage sites.

[32] After the conclusion of our fieldwork, the Bureau submitted documentation requesting the closure of our PII inventory recommendation. This documentation included an updated PII inventory and standard operating procedure document. We will analyze the steps taken by the Bureau to close this recommendation as part of our audit follow-up process.

[33] The detailed results of our follow-up work in this area will be transmitted to the Bureau under a separate, restricted cover due to the sensitive nature of the information.

[34] U.S. Department of Homeland Security, *FY 2019 CIO FISMA Metrics*, Version 1, December 2018.

OIG Comment

We believe that the actions described by the Bureau are responsive to our recommendation. We plan to follow up on the Bureau's actions to ensure that the recommendation is fully addressed.

Security Training

FISMA requires agencies to develop an information security program that provides security awareness training to personnel, including contractors, who support the operations and assets of the organization, as well as role-based training for individuals with significant information security responsibilities. NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program* (SP 800-50), notes that, in general, people are one of the weakest links in attempting to secure agency systems and networks. As such, a robust, enterprisewide security awareness and training program is paramount to ensure that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them.

A key component of an enterprisewide security training program is the assurance that individuals with significant security responsibilities have the required knowledge, skills, and abilities to perform their roles within the organization. The Federal Cybersecurity Workforce Assessment Act of 2015 requires federal agencies to conduct and report to Congress a baseline assessment of their existing workforce.[35] To assist in implementing these requirements, NIST published the *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework* (NICE Framework) in August 2017. The framework provides a resource to support a workforce capable of meeting an organization's cybersecurity needs, providing guidance for leaders to better understand, inventory, and track strengths and gaps in their cybersecurity workforce's knowledge, skills, and abilities. Further, the framework organizes individuals with security responsibilities into seven general categories: analyze, collect and operate, investigate, operate and maintain, oversee and govern, protect and defend, and securely provision. These general categories are then associated with specialty areas. Both general categories and specialty areas are used to identify work roles that can be used to tailor training needs for staff, depending on which functions they perform. In addition, NIST guidance identifies that agencies could use a needs assessment to determine their awareness and training needs. NIST SP 800-50 states that a needs assessment can provide justification for management to allocate adequate resources to meet identified awareness and training needs.

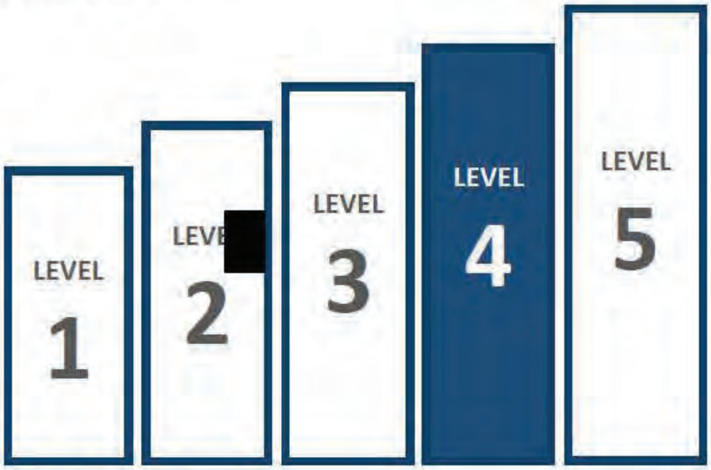
In accordance with FISMA requirements, the Bureau's *Cybersecurity Awareness and Training Process* document (CS-P-02) states that all employees and contractors with access to agency information systems must receive security awareness training before being permitted access to the Bureau network and each year thereafter. The policy also requires that role-based training be provided for individuals with significant security responsibilities and that records of awareness and role-based training be maintained.

[35] Federal Cybersecurity Workforce Assessment Act of 2015, Title III of Pub. L. No. 114-113, 129 Stat. 2242, 2975 (2015) (codified at 5 U.S.C. § 301 note).

Current Security Posture

We found that the Bureau has matured its security awareness and training program from level 3 in 2018 to a level-4 (*managed and measurable*) maturity, which represents an effective level of maturity (figure 10). This year, we found that the Bureau has strengthened its cybersecurity training program in several areas. For example, the Bureau leverages an automated security awareness training solution, conducts agencywide phishing campaigns, and provides individuals who have significant security responsibilities with specialized security training before they are provided access to information or perform assigned duties, and periodically thereafter. Officials stated that these changes are a part of the Bureau's grassroots campaign to increase security awareness throughout the agency. Moreover, in 2019 the Bureau improved its mapping of IT employee types to the respective NICE Framework training category.

Figure 10. Security Training, Level 4 (*Managed and Measurable*)



Source. OIG analysis.

Opportunities for Improvement

While we found that the Bureau's security training program is operating effectively at a level-4 (*managed and measurable*) maturity, we identified opportunities to improve the program. Specially, we found that the Bureau is working on an assessment of the knowledge, skills, and abilities of its workforce, particularly for those individuals with specialized security roles. Completion of this assessment will help the Bureau identify gaps that can be used as a key input to update the agency's awareness and specialized training program. As such, we are not making a recommendation in this area at this time but will continue to monitor the Bureau's progress as part of our future FISMA reviews.

Detect

The objective of the *detect* function in the Cybersecurity Framework is to implement activities to discover and identify the occurrence of cybersecurity events in a timely manner. The Cybersecurity Framework notes that continuous monitoring processes are used to detect anomalies and changes in the organization's environment of operation, maintain knowledge of threats, and ensure security control effectiveness. Examples of the assessment areas in this security function, as outlined in the IG FISMA reporting metrics, that we assessed include the Bureau's progress in developing and implementing an ISCM strategy, performing ongoing system authorizations, and using ISCM-related performance measures.

Information Security Continuous Monitoring

ISCM refers to the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Best practices for implementing ISCM are outlined in NIST Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (SP 800-137). SP 800-137 notes that a key component of an effective ISCM program is a comprehensive ISCM strategy based on risk tolerance that maintains clear visibility into assets, awareness of vulnerabilities, up-to-date threat information, and mission and business impacts.

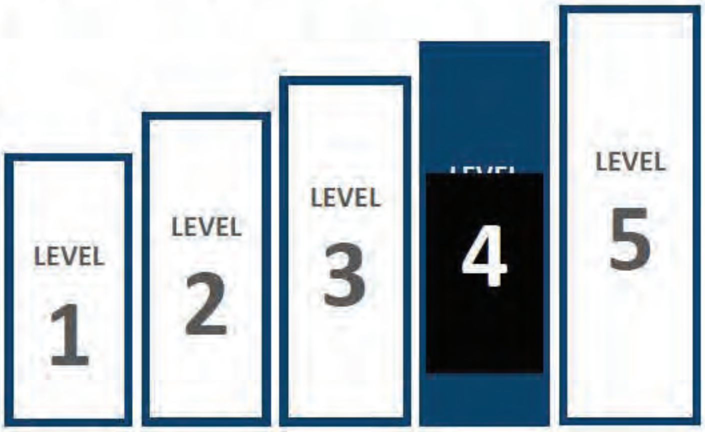
SP 800-137 emphasizes that an ISCM strategy is meaningful only within the context of broader organizational needs, objectives, or strategies, and as part of a broader risk management strategy. Once an ISCM strategy is defined, SP 800-137 notes that the next step in establishing an effective ISCM program is to establish and collect security-related metrics to support risk-based decisionmaking throughout the organization. An ISCM strategy is periodically reviewed to ensure that it sufficiently supports the organization in operating within acceptable risk tolerance levels, metrics remain relevant, and data are current and complete.

To further enhance the government's ISCM capabilities, DHS established the CDM program. A key goal of the CDM program is to provide agencies with capabilities and tools to identify cybersecurity risks on an ongoing basis, prioritize these risks based on potential effects, and enable cybersecurity personnel to mitigate the most significant problems first.

Current Security Posture

We found that the Bureau's ISCM program continues to operate at a level-4 (*managed and measurable*) maturity, which represents an effective level of maturity (figure 11). The Bureau has made several improvements to its ISCM program. For instance, the agency has enhanced the functionality of its security information and event-monitoring tool by using storyboards to describe attack scenarios and by monitoring for instances of large files being transferred.[36] Additionally, the Bureau has implemented continuous monitoring tools that perform spam filtering and vulnerability management for its network devices.

Figure 11. ISCM, Level 4 (*Managed and Measurable*)



Source. OIG analysis.

Opportunities for Improvement

While the Bureau's ISCM program is operating at a level-4 (*managed and measurable*) maturity, we identified opportunities to improve the program. First, as noted earlier in our report, the agency has not established a formal HVA program and identified its HVAs, in accordance with DHS and OMB guidance.

[36] Storyboards are attack-based scenarios. The Bureau uses storyboards to describe how alerts from the Bureau's security information and event-monitoring tool are used to detect more-sophisticated attacks using the data already collected by the agency. Because of this new feature, the Bureau has configured more searches within its security information and event-monitoring tool to automatically detect and alert on the storyboards.

Once the Bureau has identified its HVAs, it will need to determine what additional security controls and activities need to be implemented for these systems, including for ISCM. For example, guidance from the Federal CIO Council notes that agencies must implement increased monitoring and analysis of relevant audit logs for all HVAs while maintaining full asset visibility and control. Because our report includes a recommendation for the Bureau to establish an overall HVA program to include specific control considerations for HVAs, we are not making a separate recommendation in this area. We will continue to monitor the Bureau's efforts to determine control requirements for its HVAs, including for ISCM, as part of our future FISMA reviews.

Second, the Bureau is integrating its ISCM strategy and supporting processes with its ERM program. As noted earlier, the Bureau has not implemented all components of its ERM program, including defining its risk appetite statement and tolerance levels. We believe that as the Bureau continues to mature its ERM program, updates will be needed to the agency's ISCM program to ensure alignment, particularly with respect to monitoring frequencies and metrics. For example, SP 800-137 notes that an organization's ISCM strategy is developed and implemented to support risk management, in accordance with organizational risk tolerance. Further, SP 800-137 states that metrics are designed and ISCM frequencies are determined to ensure that information needed to manage risk within organizational tolerances is available. Because the Bureau is implementing its ERM program, we are not making a specific recommendation in this area at this time. We will continue to monitor the Bureau's efforts to update its ISCM program to better align with ERM activities as part of our future FISMA reviews.

Finally, the Bureau could mature its ISCM program by using the tools and capabilities offered by the CDM program, where appropriate. Bureau officials stated that they are still working with DHS to integrate their ISCM tools with those offered under the CDM program. Bureau officials further stated that network connections will be established to initiate data feeds between the two agencies. Because the Bureau is relying on the milestones established by DHS for CDM implementation for small agencies, we will not make a recommendation in this area at this time. However, we will continue to monitor the Bureau's progress in implementing the capabilities of the CDM program as part of our future FISMA reviews.

Respond

The objective of the *respond* function in the Cybersecurity Framework is to implement processes to contain the impact of detected cybersecurity events. Activities include developing and implementing incident response plans and procedures, analyzing security events, and effectively communicating incident response activities. Examples of the assessment areas in this security function, as outlined in the IG FISMA reporting metrics, that we assessed include the Bureau's incident detection, analysis, handling, and reporting processes.

Incident Response

FISMA requires each agency to develop, document, and implement an agencywide information security program that includes policies and procedures for incident response. Best practices for incident response are detailed in NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide*, which notes that an incident response process consists of four main phases: preparation; detection and analysis; containment, eradication, and recovery; and postincident activity (table 5). It further notes that establishing an incident response capability should include creating an incident response policy and plan;

developing procedures for performing incident handling and reporting; and establishing relationships and lines of communications between the incident response team and other groups, both internal and external to the agency.

Table 5. Key Incident Response Phases

Incident response phase	Description
Preparation	Establish and train the incident response team and acquire the necessary tools and resources.
Detection and analysis	Detect and analyze precursors and indicators. A precursor is a sign that an incident may occur in the future, and an indicator is a sign that an incident may have occurred or is occurring currently.
Containment, eradication, and recovery	Contain an incident to limit its impact, gather and handle evidence, eliminate components of the incident, and restore affected systems to normal operations.
Postincident activity	Capture lessons learned to improve security measures and the incident response process.

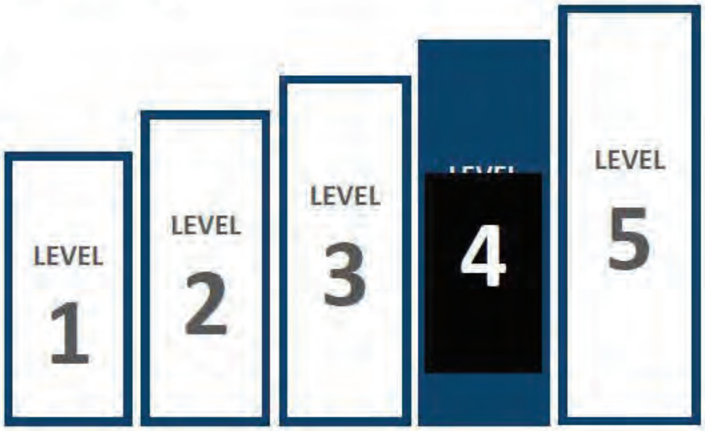
Source. NIST Special Publication 800-61, Revision 2, *Computer Security Incident Handling Guide.*

The Bureau's incident response policies and procedures address requirements and processes for incident detection, response, and reporting of information security incidents related to agency data and resources. The policies and procedures include scope, roles and responsibilities, incident notification and escalation tasks, external reporting requirements, and a threat vector taxonomy. The Bureau also coordinates with DHS in support of incident response, including reporting incidents to the United States Computer Emergency Readiness Team within an hour as required by the *US-CERT Federal Incident Notification Guidelines.*

Current Security Posture

We found that the Bureau's incident response program continues to operate at a level-4 (*managed and measurable*) maturity, which represents an effective level of maturity (figure 12). This year, the Bureau matured several incident response capabilities. For instance, the agency has deployed a data loss prevention tool, and it is using a service offered by DHS for preventing malicious traffic from affecting the agency's network. Further, since our review last year, the Bureau has begun tracking additional metrics related to the

Figure 12. Incident Response, Level 4 (*Managed and Measurable*)



Source. OIG analysis.

effectiveness of incident response processes and has created plans to further mature capabilities in this area.

Opportunities for Improvement

While the Bureau's incident response program is operating at a level-4 (*managed and measurable*) maturity, we identified opportunities to improve the program by ensuring the accuracy and consistency of cybersecurity and privacy event information captured in incident tickets. The Bureau uses tickets as the primary vehicle for documenting the characteristics of cybersecurity and privacy events and for ensuring that such events are routed to appropriate individuals for action, including the determination of whether events constitute an incident. Cybersecurity events can be generated from a number of sources, such as monitors and host-based sensors placed on the Bureau's network; internal and external logs; and reporting of suspicious activity, such as emails, by end users. Specifically, we found that internal categorization[37] of cybersecurity and privacy events was not accurately or consistently performed in incident tickets. Further, for privacy events, we identified multiple instances where the *date closed* field was left blank in incident tickets. Because of the sensitive nature of this information, the details of these issues will be transmitted to the Bureau under a separate, restricted cover.

Bureau officials noted that they employ a peer review process for cybersecurity incident tickets that should have flagged the issues we identified. Additionally, Bureau officials stated that for privacy incident tickets, personnel turnover in early 2019 contributed to the completeness issues we identified. The Bureau's *Information Security Standards* (CS-01) requires that information system security incidents be tracked and documented and that metrics be used for measuring the incident response capability within the organization. Ensuring the accuracy of information captured in security and privacy incident tickets could provide the Bureau with additional assurance that such incidents are effectively investigated and reported. In addition, the Bureau will have more accurate and comprehensive information for its incident response metrics and trend analyses.

Recommendation

We recommend that the CIO and the Chief Data Officer

6. Ensure that data captured in security and privacy incident processes and tickets are accurate, consistent, and of high quality.

Management Response

The Acting CIO concurs with this recommendation. The Acting CIO notes that the Bureau plans to make improvements in its privacy event and incident ticketing practices by performing a review of internal categorization practices to improve data quality and ensure enhanced risk mitigation ability. The Acting CIO further notes that the agency is monitoring data quality metrics and plans to make improvements to those metrics to minimize the likelihood of data quality issues occurring in the future.

[37] The Bureau's *Computer Security Incident Response Team (CSIRT) Standard Operating Procedures* notes that event categories can include denial of service, misuse, lost device, PII spillage, and suspicious email.

OIG Comment

We believe that the actions described by the Bureau are responsive to our recommendation. We plan to follow up on the Bureau's actions to ensure that the recommendation is fully addressed.

Recover

The objective of the *recover* function in the Cybersecurity Framework is to ensure that organizations maintain resilience by implementing appropriate activities to restore capabilities or infrastructure services that were impaired by a cybersecurity event. The Cybersecurity Framework outlines contingency planning processes that support timely recovery to normal operations and reduce the impact of a cybersecurity event. The IG FISMA reporting metrics focus on evaluating agency contingency planning processes. Examples of the assessment areas in this security function that we assessed include the Bureau's processes for conducting business impact analysis (BIA), developing and testing information system contingency plans, and managing contingency planning considerations related to the agency's information and communications technology (ICT) supply chain.

Contingency Planning

FISMA requires agencies to develop, document, and implement plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization. Information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption. NIST Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (SP 800-34), provides best practices for information system contingency planning.

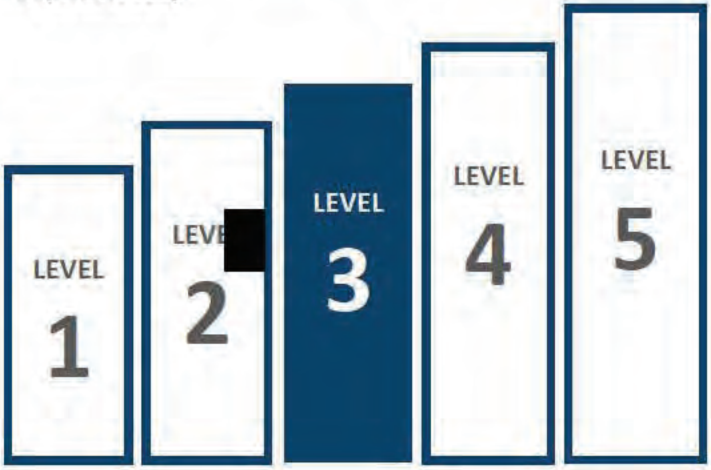
SP 800-34 notes that conducting a BIA is a key component of the information system contingency planning process and enables an organization to characterize system components, supported mission and business processes, and interdependencies. NIST SP 800-34 further states that continuity of operations functions are subject to a process-focused BIA, while federal information systems are subject to a system-focused BIA. A system-level BIA consists of three main components and can leverage the information contained in the process-focused BIA: (1) determination of mission and business processes supported by the system and associated recovery capability, (2) identification of resource requirements, and (3) identification of recovery priorities for system resources.

Another key component of an effective contingency planning program is the consideration of risk from an organization's ICT supply chain. NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (SP 800-161), highlights ICT supply chain concerns associated with contingency planning, including alternative suppliers of system components and services, denial-of-service attacks to the supply chain, and alternate delivery routes for critical system components.[38] In addition, in December 2018, the SECURE Technology Act was passed to strengthen agency supply chain risk management practices. The act establishes a Federal Acquisition Security Council to provide agencies with guidance related to mitigating supply chain risks in the procurement of IT and to establish criteria for determining which types of products pose supply chain security risks to the federal government.[39] The importance of supply chain risk management is also highlighted by its inclusion and enhanced focus in the recent update to the NIST Cybersecurity Framework.[40] For example, with respect to contingency planning, the framework notes that response and recovery planning and testing should be conducted with suppliers and third-party providers.

Current Security Posture

The Bureau's contingency planning program is operating at a level-3 (*consistently implemented*) maturity (figure 13). For instance, the Bureau has defined and communicated roles and responsibilities for contingency planning and reinforces these during newly implemented functional testing. Additionally, the Bureau has conducted an organizational-level (process-focused) BIA to determine contingency planning requirements and priorities.

Figure 13. Contingency Planning, Level 3 (*Consistently Implemented*)



Source. OIG analysis.

Opportunities for Improvement

We identified opportunities for the Bureau to mature its contingency planning program in the areas of system-level BIAs, contingency plan testing, and consideration of ICT supply chain risks. Specifically, while the Bureau has completed an organizational-level BIA, the organization has not completed system-level BIAs. NIST SP 800-34 notes that system-level BIAs should include determination of process and system criticality, outage impacts, and estimated downtime (including maximum tolerable downtime, recovery time objective, and recovery point objective), resource requirements, and recovery priorities for system resources. Bureau officials stated that they believe that the key components of a system-level BIA are included in their *Information Technology Contingency Plan* (CS-PL-01). However, we found that the plan does not cover system criticality, outage impacts, recovery priorities, and other key timings for the organization's systems. By

[38] The guidance and controls in this publication are recommended for use with high-impact systems according to Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*. However, according to NIST, because of interdependencies and individual needs, agencies may choose to apply the guidance to systems at a lower-impact level or to specific system components.

[39] At the conclusion of our fieldwork, the Federal Acquisition Security Council had not yet issued guidance related to mitigation of ICT supply chain risks.

[40] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity,* Version 1.1, April 16, 2018.

conducting system-level BIAs, the Bureau will be able to identify critical services within each system and adjust contingency planning priorities and resources, as appropriate.

We also found that the Bureau has opportunities to mature its contingency planning program through the consideration and management of ICT supply chain risks. SP 800-161 notes that many techniques used for contingency planning, such as alternative processing sites, have their own ICT supply chains and risks. Organizations should ensure that they understand and manage ICT supply chain risks and dependencies related to the contingency planning activities, as necessary. While we recognize that SP 800-161 applies to high-risk systems, with the additional governmentwide focus on supply chain risk management, we believe that the Bureau should determine the applicability of ICT supply chain risks to its environment. As the Federal Acquisition Security Council works to develop additional criteria regarding the supply chain security risks to the federal government, the Bureau has an opportunity to further enhance its contingency planning program through the consideration of these risks. While we are not making a recommendation in this area at this time, we will continue to monitor the Bureau's efforts, including its response to guidance issued by the Federal Acquisition Security Council, as part of our future FISMA reviews.

Recommendation

We recommend that the CIO

7. Ensure that system-level BIAs are conducted, as appropriate, and that the results are incorporated into contingency planning strategies and processes.

Management Response

The Acting CIO concurs with this recommendation. The Acting CIO notes that the Bureau will continue to mature its contingency management program to encompass system-level BIA, as appropriate. The Acting CIO further notes that this effort will take into consideration additional contingency planning processes, such as determination of system criticality, outage impacts, estimated downtime, resource requirements, and recovery priorities.

OIG Comment

We believe that the actions described by the Bureau are responsive to our recommendation. We plan to follow up on the Bureau's actions to ensure that the recommendation is fully addressed.

Status of Prior Years' Recommendations

As part of our 2019 FISMA audit, we reviewed the actions taken by the Bureau to address the outstanding recommendations from our prior years' FISMA reviews. Below is a summary of the status of the 10 recommendations that were open at the start of our 2019 FISMA audit (table 6). Based on corrective actions taken by the Bureau, we are closing 3 prior recommendations related to data protection and privacy, incident response, and contingency planning. The remaining 7 recommendations related to risk management, configuration management, and identity and access management will remain open. We will update the status of these recommendations in our upcoming semiannual report to Congress and continue to monitor the Bureau's progress in addressing our open recommendations as a part of our future FISMA reviews.

Table 6. Status of Prior Years' Recommendations

Recommendation	Status	Disposition
Risk management		
In our 2016 FISMA audit report, we recommended that the CIO, in conjunction with the Chief Operating Officer, evaluate options and develop an agencywide insider threat program to include (1) a strategy to raise organizational awareness, (2) an optimal organizational structure, and (3) integration of incident response capabilities, such as ongoing activities around data loss prevention.	Open	The Bureau has developed a communications plan to raise organizational awareness about insider threats. The plan defines organization structures and outlines the current capabilities that support the insider threat program from a people, processes, and technology perspective. However, the Bureau has not fully implemented its data loss prevention tool.
In our 2017 FISMA audit report, we recommended that the Chief Risk Officer continue to work with divisions across the Bureau to ensure that a risk appetite statement and associated risk tolerance levels are defined and used to develop and maintain an agencywide risk profile.	Open	Although the Bureau has made progress in establishing its ERM program, it has not yet finalized its risk appetite statement or risk tolerance levels.

Recommendation	Status	Disposition
Configuration management		
In our 2014 FISMA audit report, we recommended that the CIO strengthen the Bureau’s vulnerability management practices by implementing an automated solution and process to periodically assess and manage database and application-level security configurations.	Open	The Bureau has implemented an automated solution for assessing application-level security configurations for web applications but has not done so for assessing and managing database security configurations.
In our 2018 FISMA audit report, we recommended that the CIO strengthen configuration management processes by (1) remediating configuration-related vulnerabilities in a timely manner and (2) ensuring that optimal resources are allocated to perform vulnerability remediation activities.	Open	The Bureau still has numerous critical and high-risk vulnerabilities that were not remediated in a timely manner. Further, our operating system–level scanning identified a number of critical and high-risk vulnerabilities that had also been identified by the Bureau’s internal vulnerability scans months earlier.
In our 2018 FISMA audit report, we recommended that the CIO develop and implement a process to ensure the timely application of patches and security updates for Bureau-issued mobile phones.	Open	Bureau officials informed us that they are updating policy and implementing a tool to enforce the application of current patches for mobile phones.
Identity and access management		
In our 2017 FISMA audit report, we recommended that the CIO develop and implement a tiered approach for implementing multifactor authentication that considers system risk levels and user roles and uses lessons learned to inform broader adoption.	Open	The Bureau implemented several technical solutions that in totality did not completely meet NIST level of assurance 4 multifactor authentication.
In our 2018 FISMA audit report, we recommend that the CIO determine whether established processes and procedures for management of user-access agreements and rules-of-behavior forms for privileged users are effective and adequately resourced and make changes as needed.	Open	The Bureau is not consistently following its policies and procedures to ensure that access agreements and associated rules of behavior are completed prior to access being granted to systems.

Recommendation	Status	Disposition
Data protection and privacy		
In our 2018 FISMA audit report, we recommended that the CIO ensure that the Bureau's existing ISCM approach is implemented for an internal collaboration tool to appropriately restrict and monitor access.	Closed	The Bureau has taken actions to strengthen the security of its internal collaboration tool, including using continuous monitoring processes to restrict access and monitor logs.
Incident response		
In our 2017 FISMA audit report, we recommended that the CIO ensure applicable alerts and logs from applications residing in the Bureau's new cloud computing environment are uploaded to the agency's central automated solution, which is used to detect and analyze incidents.	Closed	The Bureau has ensured that logs from its cloud computing environment are uploaded to its central automated solution.
Contingency planning		
In our 2016 FISMA audit report, we recommended that the CIO strengthen the Bureau's contingency program by performing an agencywide BIA and updating the agency's continuity of operations plan and IT contingency plan to reflect the results of the BIA and the current operating environment of the Bureau.	Closed	The Bureau conducted an organizational-level BIA and updated its strategy and planning documentation accordingly.

Appendix A: Scope and Methodology

Our specific audit objectives, based on FISMA requirements, were to evaluate the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. To accomplish our objectives, we reviewed the effectiveness of the Bureau's information security program across the five function areas outlined in DHS's IG FISMA reporting metrics: *identify*, *protect*, *detect*, *respond*, and *recover*. These five function areas consist of eight security domains: risk management, configuration management, identity and access management, data protection and privacy, security training, ISCM, incident response, and contingency planning.

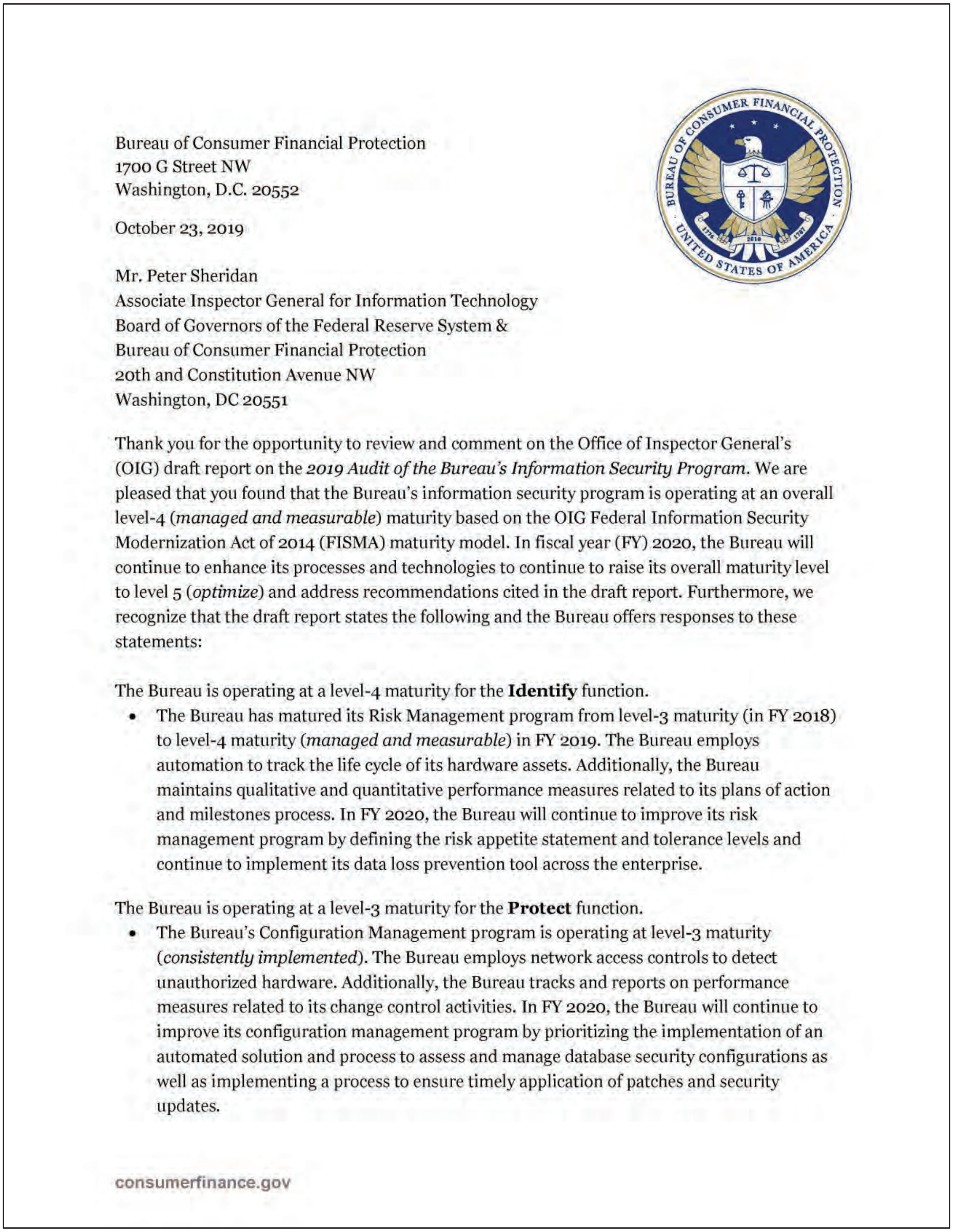
To assess the Bureau's information security program, we interviewed Bureau management and staff; analyzed security policies, procedures, and documentation; performed vulnerability scanning at the network, operating system, and database levels for select systems;[41] and observed and tested specific security processes and controls. We used commercially available software to perform data analytics to support our effectiveness conclusions for specific metrics in multiple security domains. The data we analyzed were related to three of the Bureau's cloud-based systems.

To rate the maturity of the Bureau's information security program and functional areas, we used the scoring methodology defined in DHS's IG FISMA reporting metrics. The maturity ratings are determined by a simple majority, where the most frequent level (that is, the mode) across the metrics serves as the overall rating.

We performed our fieldwork from May 2019 to September 2019. We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[41] The detailed results of our technical testing will be transmitted to the Bureau under a separate, restricted cover due to the sensitive nature of the information.

Appendix B: Management Response



Bureau of Consumer Financial Protection
1700 G Street NW
Washington, D.C. 20552

October 23, 2019

Mr. Peter Sheridan
Associate Inspector General for Information Technology
Board of Governors of the Federal Reserve System &
Bureau of Consumer Financial Protection
20th and Constitution Avenue NW
Washington, DC 20551

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) draft report on the *2019 Audit of the Bureau's Information Security Program*. We are pleased that you found that the Bureau's information security program is operating at an overall level-4 (*managed and measurable*) maturity based on the OIG Federal Information Security Modernization Act of 2014 (FISMA) maturity model. In fiscal year (FY) 2020, the Bureau will continue to enhance its processes and technologies to continue to raise its overall maturity level to level 5 (*optimize*) and address recommendations cited in the draft report. Furthermore, we recognize that the draft report states the following and the Bureau offers responses to these statements:

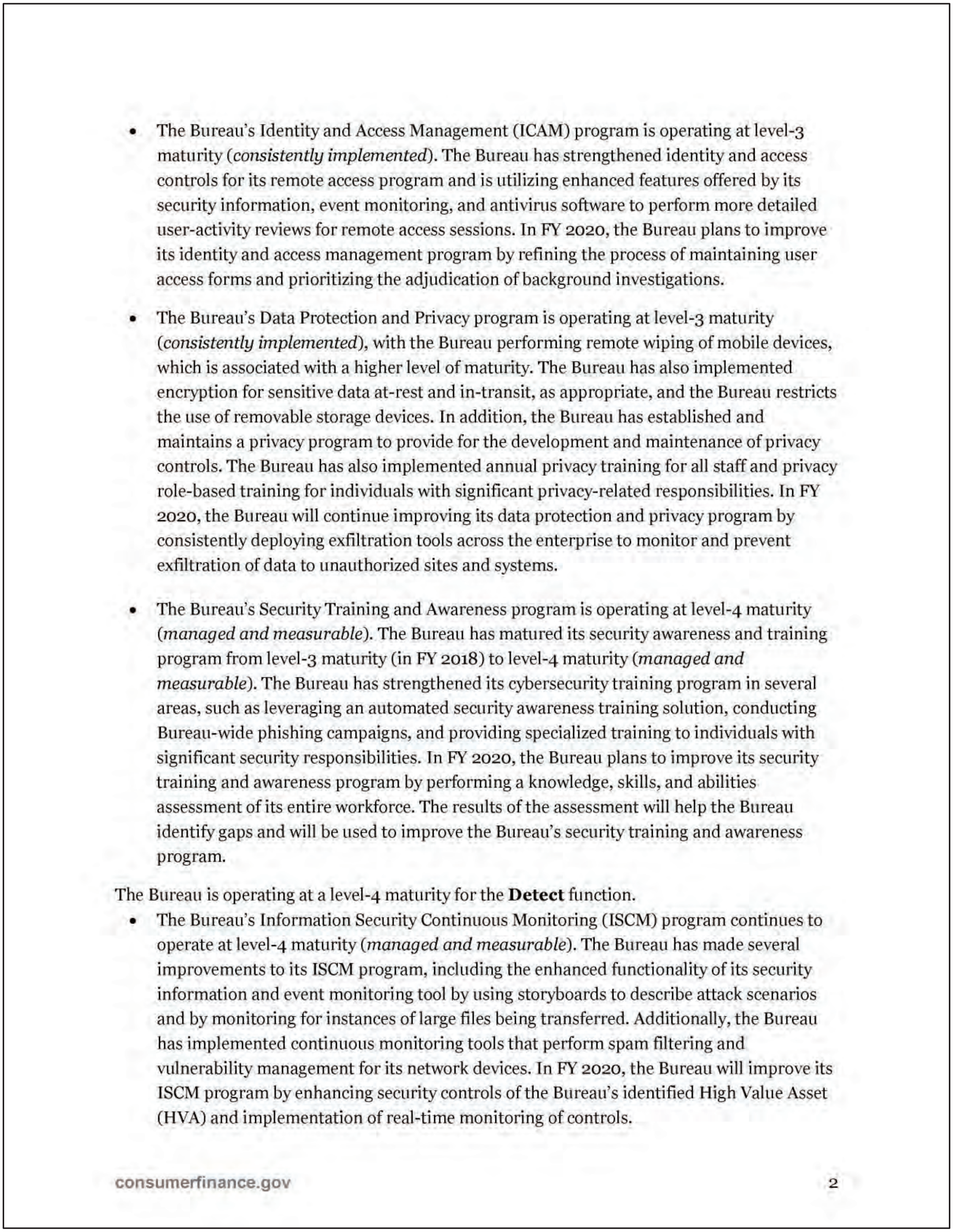
The Bureau is operating at a level-4 maturity for the **Identify** function.

- The Bureau has matured its Risk Management program from level-3 maturity (in FY 2018) to level-4 maturity (*managed and measurable*) in FY 2019. The Bureau employs automation to track the life cycle of its hardware assets. Additionally, the Bureau maintains qualitative and quantitative performance measures related to its plans of action and milestones process. In FY 2020, the Bureau will continue to improve its risk management program by defining the risk appetite statement and tolerance levels and continue to implement its data loss prevention tool across the enterprise.

The Bureau is operating at a level-3 maturity for the **Protect** function.

- The Bureau's Configuration Management program is operating at level-3 maturity (*consistently implemented*). The Bureau employs network access controls to detect unauthorized hardware. Additionally, the Bureau tracks and reports on performance measures related to its change control activities. In FY 2020, the Bureau will continue to improve its configuration management program by prioritizing the implementation of an automated solution and process to assess and manage database security configurations as well as implementing a process to ensure timely application of patches and security updates.

consumerfinance.gov



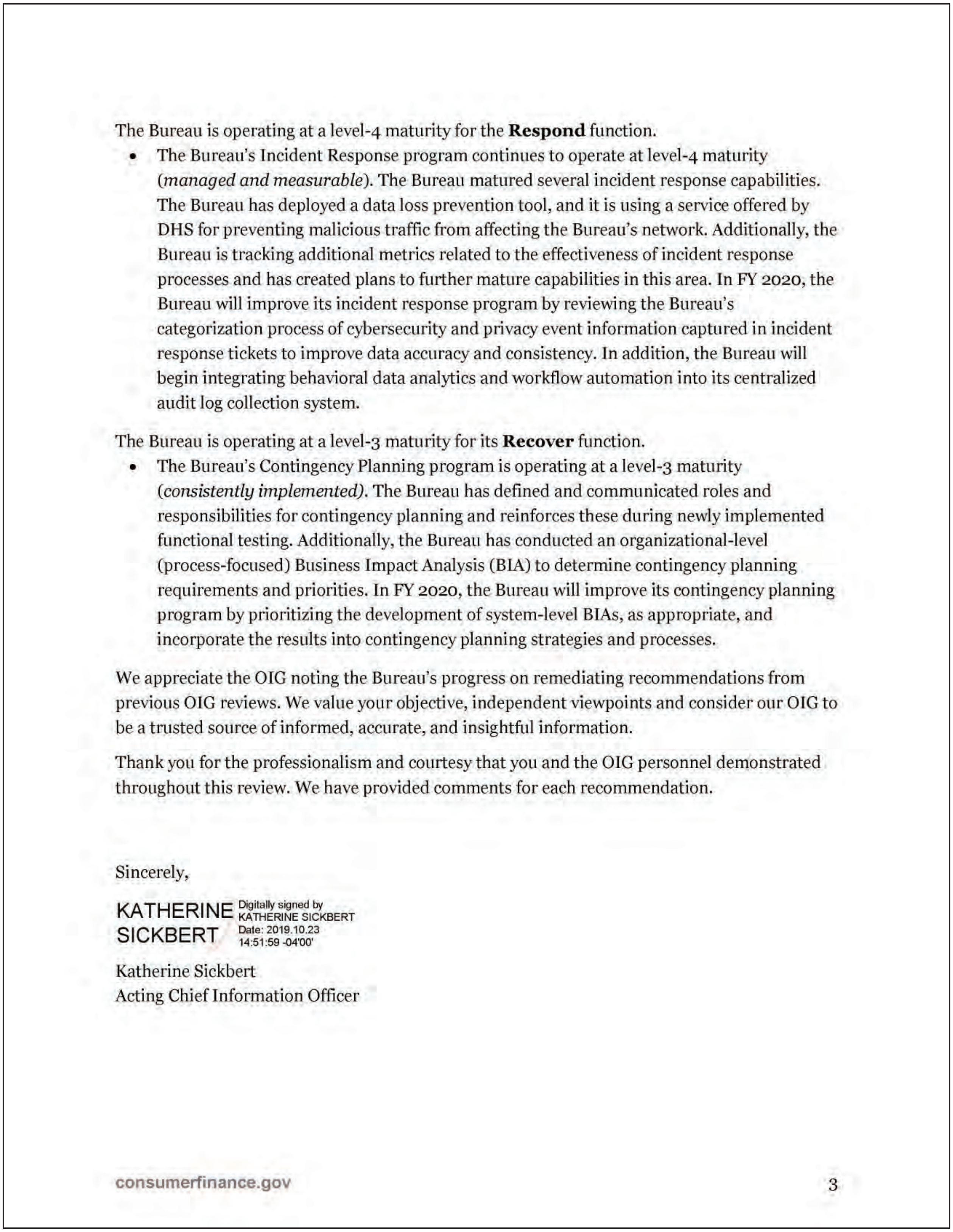
- The Bureau's Identity and Access Management (ICAM) program is operating at level-3 maturity (*consistently implemented*). The Bureau has strengthened identity and access controls for its remote access program and is utilizing enhanced features offered by its security information, event monitoring, and antivirus software to perform more detailed user-activity reviews for remote access sessions. In FY 2020, the Bureau plans to improve its identity and access management program by refining the process of maintaining user access forms and prioritizing the adjudication of background investigations.

- The Bureau's Data Protection and Privacy program is operating at level-3 maturity (*consistently implemented*), with the Bureau performing remote wiping of mobile devices, which is associated with a higher level of maturity. The Bureau has also implemented encryption for sensitive data at-rest and in-transit, as appropriate, and the Bureau restricts the use of removable storage devices. In addition, the Bureau has established and maintains a privacy program to provide for the development and maintenance of privacy controls. The Bureau has also implemented annual privacy training for all staff and privacy role-based training for individuals with significant privacy-related responsibilities. In FY 2020, the Bureau will continue improving its data protection and privacy program by consistently deploying exfiltration tools across the enterprise to monitor and prevent exfiltration of data to unauthorized sites and systems.

- The Bureau's Security Training and Awareness program is operating at level-4 maturity (*managed and measurable*). The Bureau has matured its security awareness and training program from level-3 maturity (in FY 2018) to level-4 maturity (*managed and measurable*). The Bureau has strengthened its cybersecurity training program in several areas, such as leveraging an automated security awareness training solution, conducting Bureau-wide phishing campaigns, and providing specialized training to individuals with significant security responsibilities. In FY 2020, the Bureau plans to improve its security training and awareness program by performing a knowledge, skills, and abilities assessment of its entire workforce. The results of the assessment will help the Bureau identify gaps and will be used to improve the Bureau's security training and awareness program.

The Bureau is operating at a level-4 maturity for the **Detect** function.

- The Bureau's Information Security Continuous Monitoring (ISCM) program continues to operate at level-4 maturity (*managed and measurable*). The Bureau has made several improvements to its ISCM program, including the enhanced functionality of its security information and event monitoring tool by using storyboards to describe attack scenarios and by monitoring for instances of large files being transferred. Additionally, the Bureau has implemented continuous monitoring tools that perform spam filtering and vulnerability management for its network devices. In FY 2020, the Bureau will improve its ISCM program by enhancing security controls of the Bureau's identified High Value Asset (HVA) and implementation of real-time monitoring of controls.



The Bureau is operating at a level-4 maturity for the **Respond** function.

- The Bureau's Incident Response program continues to operate at level-4 maturity (*managed and measurable*). The Bureau matured several incident response capabilities. The Bureau has deployed a data loss prevention tool, and it is using a service offered by DHS for preventing malicious traffic from affecting the Bureau's network. Additionally, the Bureau is tracking additional metrics related to the effectiveness of incident response processes and has created plans to further mature capabilities in this area. In FY 2020, the Bureau will improve its incident response program by reviewing the Bureau's categorization process of cybersecurity and privacy event information captured in incident response tickets to improve data accuracy and consistency. In addition, the Bureau will begin integrating behavioral data analytics and workflow automation into its centralized audit log collection system.

The Bureau is operating at a level-3 maturity for its **Recover** function.

- The Bureau's Contingency Planning program is operating at a level-3 maturity (*consistently implemented)*. The Bureau has defined and communicated roles and responsibilities for contingency planning and reinforces these during newly implemented functional testing. Additionally, the Bureau has conducted an organizational-level (process-focused) Business Impact Analysis (BIA) to determine contingency planning requirements and priorities. In FY 2020, the Bureau will improve its contingency planning program by prioritizing the development of system-level BIAs, as appropriate, and incorporate the results into contingency planning strategies and processes.

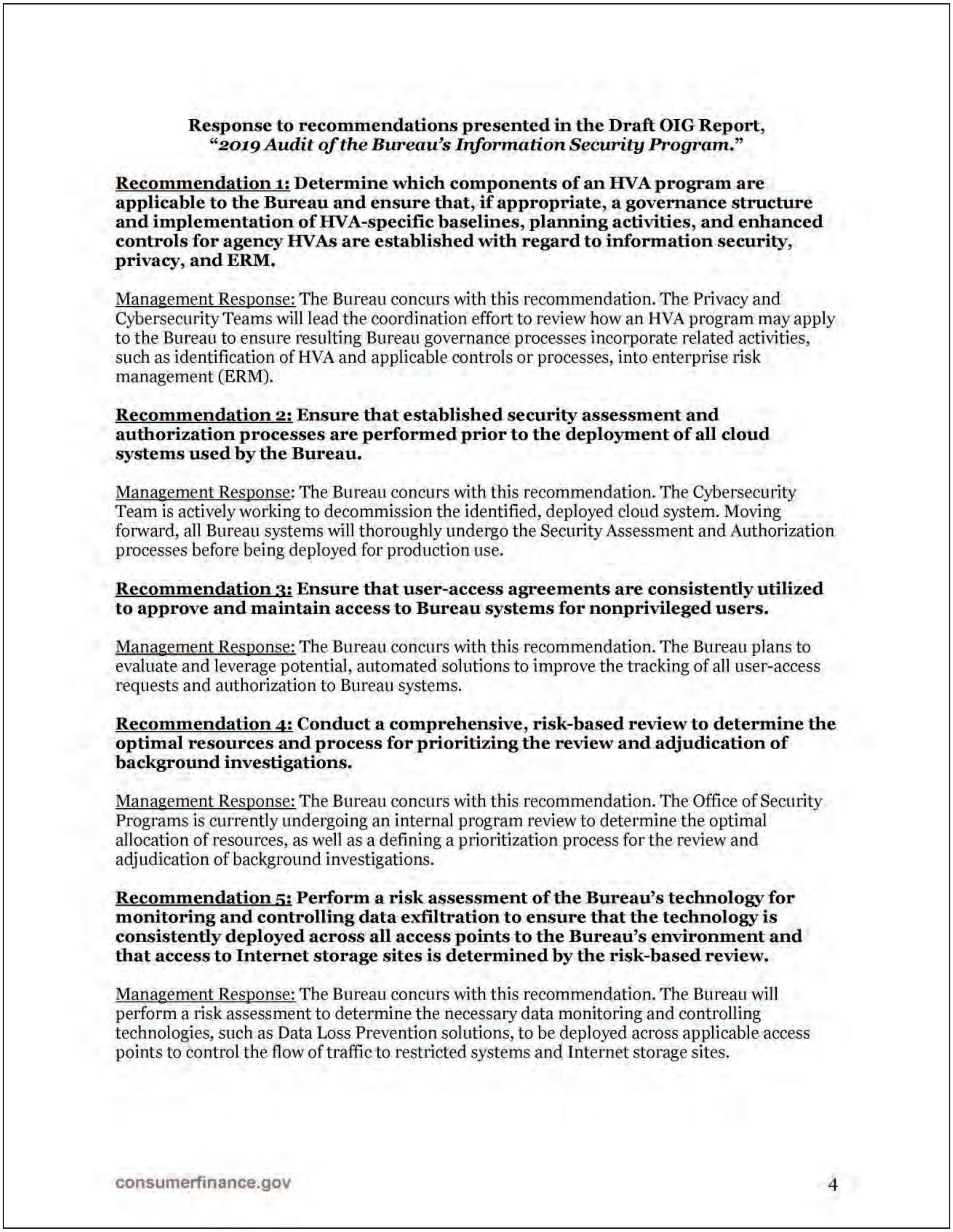
We appreciate the OIG noting the Bureau's progress on remediating recommendations from previous OIG reviews. We value your objective, independent viewpoints and consider our OIG to be a trusted source of informed, accurate, and insightful information.

Thank you for the professionalism and courtesy that you and the OIG personnel demonstrated throughout this review. We have provided comments for each recommendation.

Sincerely,

KATHERINE SICKBERT
Digitally signed by KATHERINE SICKBERT
Date: 2019.10.23 14:51:59 -04'00'

Katherine Sickbert
Acting Chief Information Officer



Response to recommendations presented in the Draft OIG Report, "*2019 Audit of the Bureau's Information Security Program.*"

<u>Recommendation 1:</u> Determine which components of an HVA program are applicable to the Bureau and ensure that, if appropriate, a governance structure and implementation of HVA-specific baselines, planning activities, and enhanced controls for agency HVAs are established with regard to information security, privacy, and ERM.

<u>Management Response:</u> The Bureau concurs with this recommendation. The Privacy and Cybersecurity Teams will lead the coordination effort to review how an HVA program may apply to the Bureau to ensure resulting Bureau governance processes incorporate related activities, such as identification of HVA and applicable controls or processes, into enterprise risk management (ERM).

<u>Recommendation 2:</u> Ensure that established security assessment and authorization processes are performed prior to the deployment of all cloud systems used by the Bureau.

<u>Management Response</u>: The Bureau concurs with this recommendation. The Cybersecurity Team is actively working to decommission the identified, deployed cloud system. Moving forward, all Bureau systems will thoroughly undergo the Security Assessment and Authorization processes before being deployed for production use.

<u>Recommendation 3:</u> Ensure that user-access agreements are consistently utilized to approve and maintain access to Bureau systems for nonprivileged users.

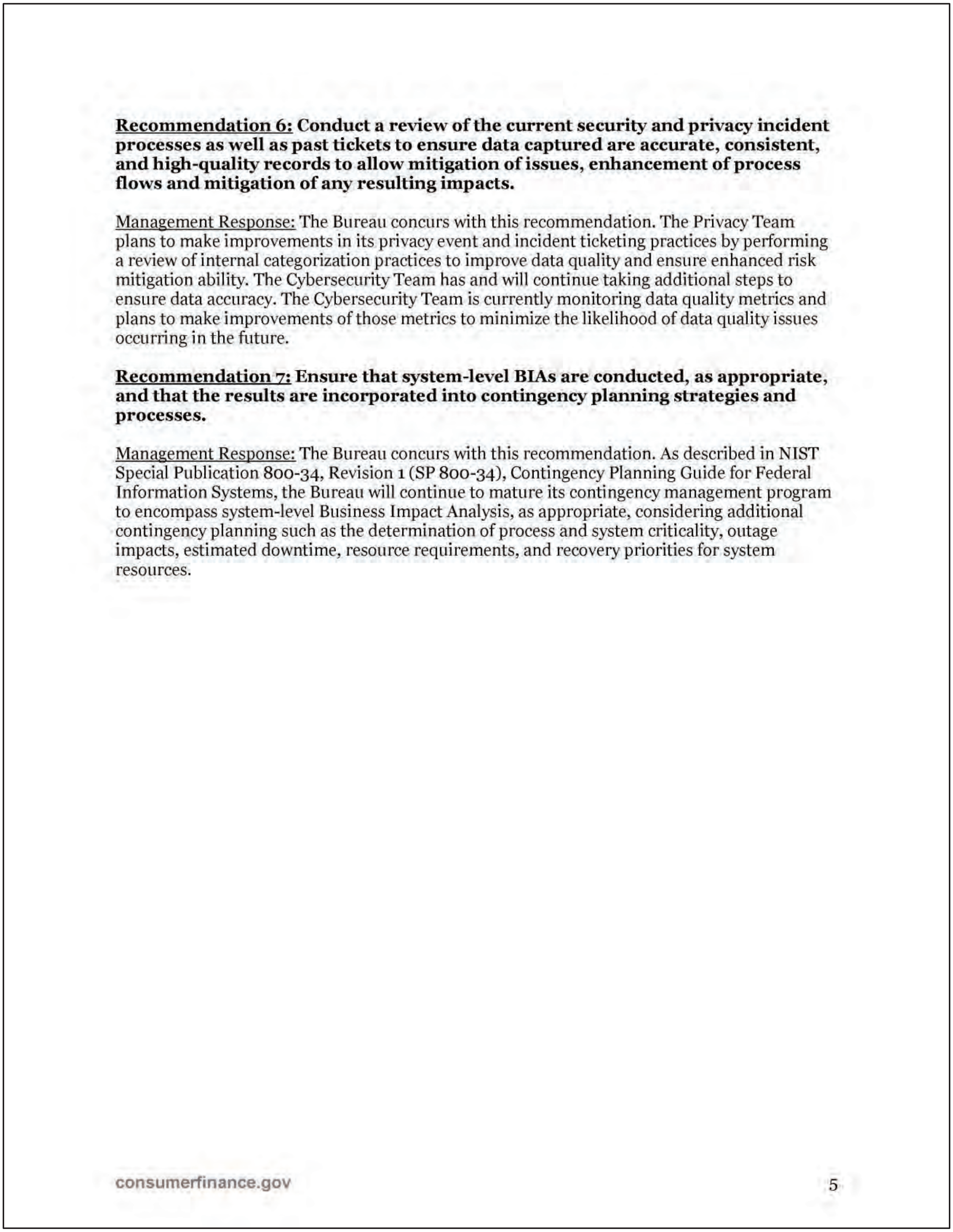
<u>Management Response:</u> The Bureau concurs with this recommendation. The Bureau plans to evaluate and leverage potential, automated solutions to improve the tracking of all user-access requests and authorization to Bureau systems.

<u>Recommendation 4:</u> Conduct a comprehensive, risk-based review to determine the optimal resources and process for prioritizing the review and adjudication of background investigations.

<u>Management Response:</u> The Bureau concurs with this recommendation. The Office of Security Programs is currently undergoing an internal program review to determine the optimal allocation of resources, as well as a defining a prioritization process for the review and adjudication of background investigations.

<u>Recommendation 5:</u> Perform a risk assessment of the Bureau's technology for monitoring and controlling data exfiltration to ensure that the technology is consistently deployed across all access points to the Bureau's environment and that access to Internet storage sites is determined by the risk-based review.

<u>Management Response:</u> The Bureau concurs with this recommendation. The Bureau will perform a risk assessment to determine the necessary data monitoring and controlling technologies, such as Data Loss Prevention solutions, to be deployed across applicable access points to control the flow of traffic to restricted systems and Internet storage sites.



<u>Recommendation 6:</u> Conduct a review of the current security and privacy incident processes as well as past tickets to ensure data captured are accurate, consistent, and high-quality records to allow mitigation of issues, enhancement of process flows and mitigation of any resulting impacts.

<u>Management Response:</u> The Bureau concurs with this recommendation. The Privacy Team plans to make improvements in its privacy event and incident ticketing practices by performing a review of internal categorization practices to improve data quality and ensure enhanced risk mitigation ability. The Cybersecurity Team has and will continue taking additional steps to ensure data accuracy. The Cybersecurity Team is currently monitoring data quality metrics and plans to make improvements of those metrics to minimize the likelihood of data quality issues occurring in the future.

<u>Recommendation 7:</u> Ensure that system-level BIAs are conducted, as appropriate, and that the results are incorporated into contingency planning strategies and processes.

<u>Management Response:</u> The Bureau concurs with this recommendation. As described in NIST Special Publication 800-34, Revision 1 (SP 800-34), Contingency Planning Guide for Federal Information Systems, the Bureau will continue to mature its contingency management program to encompass system-level Business Impact Analysis, as appropriate, considering additional contingency planning such as the determination of process and system criticality, outage impacts, estimated downtime, resource requirements, and recovery priorities for system resources.

Abbreviations

ATO	authorization to operate
BIA	business impact analysis
Bureau	Bureau of Consumer Financial Protection
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
DHS	U.S. Department of Homeland Security
ERM	enterprise risk management
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
HVA	high-value asset
ICAM	identity, credential, and access management
ICT	information and communications technology
IG	Inspector General
ISCM	information security continuous monitoring
IT	information technology
NICE Framework	*National Initiative for Cybersecurity Education Cybersecurity Workforce Framework*
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PII	personally identifiable information
PIV	personal identity verification
SA&A	security assessment and authorization
SECURE Technology Act	Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act of 2018
SP 800-34	Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
SP 800-39	Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*
SP 800-50	Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*

SP 800-53	Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
SP 800-122	Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*
SP 800-137	Special Publication 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
SP 800-161	Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*

Report Contributors

Khalid Hasan, Senior OIG Manager
Andrew Gibson, OIG Manager
Jeff Woodward, Senior IT Auditor
Kaneisha Johnson, IT Auditor
LaToya Holt, Senior Auditor
Emily Martin, IT Auditor
Justin Byun, IT Audit Intern
Fay Tang, Statistician
Alexander Karst, Senior Information Systems Analyst
Peter Sheridan, Assistant Inspector General for Information Technology

Contact Information

General

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551

Phone: 202-973-5000
Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov

OIG

Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, web form, phone, or fax.

OIG Hotline
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551

Phone: 800-827-3340
Fax: 202-973-5044

‹ Back to Announcements (b) (6) Search

Introducing Cyber Wise Security Tips: Increased cybersecurity Threat from Abroad

(b) (6)

Following the US strike on Iranian IRGC-Quds Force commander earlier this month, Iran conducted retaliatory attacks against U.S. and allied forces. The US Cybersecurity & Infrastructure Security Agency (CISA) has issued threat alerts notifying agencies to expect an increase in cyber activity coming from the middle east region as tensions between the US and Iran continue to escalate. Previous Homeland-based plots have included, among other things, scouting against infrastructure targets, assassination attempt against the Ambassador to Saudi Arabia in 2011, and cyber enabled attacks against a range of U.S.-based targets.

The FBI, DHS, and NCTC advise federal, state, local, tribal, and territorial government counterterrorism, cyber, and law enforcement officials, and private sector partners, to remain vigilant in the event of a potential Iran-directed threat to US-based individuals, facilities, and networks consistent with previously observed covert surveillance and possible pre-operational activity.

In response, the CFPB Cybersecurity team will be issuing regular updates on increased threats, tips to help keep your system secure, and information on how to spot potential attacks.

How Can You Help?

- Report suspicious activity to local law enforcement who are best to offer specific details on terroristic indicators

• Report suspicious activity or information about a threat, including online activity, to fusion centers or through proper Bureau channels
• Remain vigilant in spotting potential targeted phishing attacks coming from Iranian threat actors attempting to get you to click on a link and gain access into your system

Be Prepared
• Be prepared for a cyber incident with an offline backup, an incident response plan, and know who you are calling for help. For more information visit CISA.gov or the CFPB internal wiki
• Be responsible for your personal safety. Know where emergency exits and security personnel are located. Carry emergency contact and special needs information with you
• Connect, Plan, Train, and Report to prepare businesses & employees. Security resources can be accessed through the DHS's Hometown Security Campaign

(b) (6) [redacted]

❮ Back to Announcements

Search

Cyber Wise Security Tip: Detect & Remediate Ransomware Attacks

(b) (6) [redacted]

Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it. Typically, these attacks state that the user's files have been encrypted and user is told that unless a ransom is paid, access will not be restored. The ransom demanded from individuals varies greatly but is frequently $200–$400 dollars and must be paid in virtual currency, such as Bitcoin.

If Ransomware is observed on a CFPB computer – **Never pay the fine!**

The Bureau backs up all user files and systems every day so there is little threat of any files being lost. Power off your machine, notify the CFPB Computer Security Incident Response Team (CSIRT) and bring it to the Service Desk. They will remove the ransomware and restore your files.

Signs your system may have been infected by Ransomware:

- Your web browser or desktop is locked with a message about how to pay to unlock your system and/or your file directories contain a "ransom note" file that is usually a .txt file
- All of your files have a new file extension appended to the filenames.

Examples of Ransomware file extensions: .ecc, .ezz, .exx, .zzz, .xyz, .aaa, .abc, .ccc, .vvv, .xxx, .ttt, .micro, .encrypted, .locked, .crypto, _crypt, .crinf, .r5a, .XRNT, .XTBL, .crypt, .R16M01D05, .pzdc, .good, .LOL!, .OMG!, .RDM, .RRK, .encryptedRSA, .crjoker, .EnCiPhErEd, .LeChiffre, .keybtc@inbox_com, .0x0, .bleep, .1999, .vault, .HA3, .toxcrypt, .magic, .SUPERCRYPT, .CTBL, .CTB2, .locky or 6-7 length extension consisting of random characters

‹ Back to Announcements (b) (6) Search

Cyber Wise Security Tip: How to Detect and Prevent Social Engineering Attacks

(b) (6)

Depending on the circumstances, an unexpected email, phone call, or other message requesting sensitive data may not always raise a red flag — but it should. By pretending to be a trusted contact or using personalized details, hackers can manipulate victims into sharing personal or Department information. They may pose as a fellow Bureau employee, Service Desk support, employment recruiter, vendor or subcontractor, friend, or even senior Bureau leadership.

This approach, known as social engineering, exploits normal human interactions, emotions, and trust. Spear phishing via email or social media, "vishing" (voice phishing), and "smishing" (SMS phishing) are the most frequently used methods of social engineering, but there are many other tactics hackers use, from baiting to tailgating and scareware to honey traps.

A recent attack combined social engineering with exploitation of technical vulnerabilities. After using a bug to hack an individual's Gmail account, the attacker attached malware to a nearly complete email in the drafts folder and hit send. The email was particularly convincing because it was sent from a legitimate account, written in the hacked individual's own voice, and contained content relevant to the recipient. Social engineering methods will continue to increase in complexity and prevalence as attackers find new ways to appear trustworthy to their victims.

Given the nature of our work, Bureau employees are particularly valuable targets for social engineering attacks. Take the following steps to protect yourself and the Bureau from social engineering attempts:

1. Think before you share personal or Bureau information with anyone.

Remember, never share your login credentials, security clearance status, or potentially sensitive details about your work. On social media, don't use geo-tagging or post the names of businesses you have accounts with.

2. Use caution when answering any unsolicited phone calls, emails, or other online messages from individuals asking for your information or featuring a call to action.

3. Before providing any information, verify the requestor's identity directly with the company they say they're with. Use publicly available contact information instead of a link, email address, or phone number provided by the requestor.

4. Contact (b) (6) [redacted] if you suspect you or others have been targeted by a social engineering attack at the Bureau.

‹ Back to Announcements (b) (6) Search

Cyber Wise Security Tip: Beware of the Web Extensions You Add

(b) (6)

Recently web browsers Google Chrome and Mozilla's Firefox reported taking several hundred web extensions from their web stores for practicing risky or fraudulent behavior.

Google reportedly took down 500 extensions, "that researchers discovered were stealing browsing data and executing click fraud and malvertising after installing themselves on the computers of millions of users." Full article available here.

Stay CyberWise by following the Web Extensions best practices:

- Install as few extensions as possible and, despite the above, only from official web stores.
- Check the reviews and feedback from others who have installed the extension.
- Pay attention to the developer’s reputation and how responsive they are to questions and how frequently they post version updates.
- Study the permissions they ask for (in Chrome, Settings> Extensions> Details) and check they’re in line with the features of the extension. And if these permissions change, be suspicious.

‹ Back to Announcements (b) (6) Search

Cyber Wise Security Tip: Mobile Device Security 201

Have you ever stopped to consider how secure or safe your device is?

(b) (6)

These days it seems like everyone has at least one if not two mobile devices. These convenient little devices go everywhere with us. They enable us to conveniently connect to several different networks and services based on proximity and access. We can quickly check email, text messages, social media, bank and credit card accounts, watch movies and other media at the drop of a dime.

How sure are you that if you lost your phone tomorrow some unauthorized person won't be able to access your personal information? If you have a CFPB issued mobile device, are you doing your part to protect the Bureau network data and resources?

With the ability to connect to many different data resources, comes great responsibility.

Here are a few tips to keep your device secure:

Enable fingerprint logins for your device
Your fingerprint is much more complex and harder to crack than any strong password you can create. Also, it's hard to forget your fingerprint.

Pro-tip: Use your fingerprint (something you have) *with* a complex password (something you know) for multi-factor authentication. Multi-factor authentication requires at least two different forms of identification verification, so even if your device is lost, the criminals are far less likely to pull any info from you before you report the device stolen to our Service Desk.

Be wary of which apps with access to your location. Disable location services when you can

Many apps request permission to access your location based service (aka GPS) available in most smart devices. Be wary of who you allow to have this. An app that has this access permission, but does not provide updates to their app can introduce security risks to you.

Consider remote wiping software

Most smart phones come with the ability (check your device settings) for the data to be erased from a remote location. In order to prevent your data from getting into the wrong hands, you may want to look into how your device remote wipe technology works before it's too late.

Back up your data. Early and often.

Hopefully you will never need to wipe your data due to a , however you should be backing your data up on a hard drive or onto your cloud account (which should have strong passphrase regularly.

For more Cyber tips, check out the Cybersecurity Tip of the week wiki.

Thanks
CFPB Cybersecurity Training Team

(b) (6)

‹ Back to Announcements

Search

Cyber Wise Security Tip: Digital Spring Cleaning

With spring right around the corner, that means spring cleaning is quickly approaching. Now is the time to clean your digital devices to ensure an optimized and secure environment.

(b) (6)

(b) (5)

Refresh your passwords
Take a look at your passwords. Yes, all of them.

Do you have a habit of reusing the same password for all your accounts? That is a big risk, and increases the likelihood that your account can be compromised.
Change any account password that is not unique and be sure to include complex passwords. Complex passwords utilize the combination of numbers, special characters (ex: @, &, !, $), and both capitalize and lower case letters.

Clean desk policy
Make sure you do your best to keep a clean desk. Meaning no papers, removable media devices (ex: USB drives), or sticky notes with too much personal info is left out or in an unlocked and visible location.

Consider an email purge
This may work better for your home environment, but its still worth considering doing a mass purge of old email files that you have not looked at in more than 2 years. Do you really need all of that info?
If not, consider moving the important emails to a secure cloud drive location, or even better to a secure hard drive.

Update your devices and apps.
Make sure you have the latest version of your apps installed. If you notice

any apps you use have not released an update or patch of any kind in the last 8 months consider deleting that app.
Apps that do not regularly patch their own system vulnerabilities (every form of tech has vulnerabilities) will leave you open to feeling the effects of a breach. Uninstall that app before you have the chance to be hacked.
Consider uninstalling apps you have not used or opened in a year.

Double check your financial & social media accounts privacy and alert settings
This will be an often repeated tip.
Check all your social media and bank/credit cards to ensure your privacy settings are at a level comfortable to you.
Also take a few minutes to opt-into the transaction alerts feature, so you have the ability to spot and report fraudulent activities as soon as possible.

For more Cyber tips, check out the Cybersecurity tip of the week wiki.

Thanks
CFPB Cybersecurity Training Team

‹ Back to Announcements (b) (6) Search

Cyber Wise Security Tip: Managing your digital footprint

Have you heard that data is new gold?

(b) (6)

Continuing our digital awareness theme, here are a few things to keep in mind with any digital technology you use.

Now is the time to be as mindful as possible about your digital footprint, privacy, and data security.

Here are a few ways to manage you digital footprint:

Google yourself
Yes, seriously search for yourself using your favorite search engine and see what pops up.

Did you know that many employers look you up before hiring you?
You should know what is out there about you and decide if anything needs to be regarding the data on you.

Check your old social media accounts and posts
First, be sure to check your account privacy settings.

You should set your account to private, but if you are willing to have your account set to public, make sure everything that is publicly available is what you want to be available.
There is nothing wrong with doing a scrub of old tweets or posts that didn't age well or are inappropriate. Take a few minutes to review your posts and make sure you are proud of everything attached to your name.

Hide or modify accounts that don't allow you to delete your old accounts
Unfortunately some services don't allow you to delete your presence easily.

In cases where someone else may have uploaded your likeness, consider trying to change the name or email address attached so it doesn't follow you forever.
If possible, try swapping out an unflattering picture of yourself with a more innocent image. Hopefully with time, the image should stop appearing in search engines.

Consider use of a secondary email
Create a non-federal email account for any personal shopping or non-work related activities.
It would also be good to use that email account for sites that insist on sending you marketing or sales materials. The email should be used for any correspondence that is not related to family, friends, or school activities.
These companies are more likely to be hacked or spoofed, which can lead to the theft of your information.
So be sure to give them the fake stuff.

For more fun and insightful tips, pull up our Cybersecurity Tip of the Week wiki page.

-Cybersecurity Training Team

‹ Back to Announcements (b) (6) Search

Cyber Wise Security Tip: So your Cybersecurity department has been bugging you to create a complex password...?

(b) (6)

Yes, we keep lovingly reminding you that you need a complex or strong password. And, yes we get how annoying we can be about it.
Stay with me, there is a reason.

Did you know that more than 14 million Americans are victims of cyber related identity theft?

I bet you also didn't know that about 3.3 million of them have to bear the financial responsibilities of the fraud committed under their identity? Why exactly is it our fault? Easy to crack passwords. Repetitive passwords. Once a criminal gets one password, they try it for all your accounts.

Okay, so I can feel through this screen that you still don't believe me, so check out this Newsweek article backing me up here (promise it's not a phishing attempt).

Here is an easy way to make creating a strong AND unique password simple:

Think of a password more as a passphrase

Try piecing together a string of four or five words that are not associated, such as "hairy moose scares grandma" to create a unique set of characters that is easy recall but hard for someone to crack.
The sequence will look like 1harryM0ose@Scar3sgrandm@

Nice and easy right?

Pro-tip courtesy of Newsweek:

Try using the first letter of each word in a line or two of your favorite song or quote. Say, for instance, you're a fan of Old Town Road by Lil Nas X, which begins: "Yeah, I'm gonna take my horse to the old town road. I'm gonna ride 'til I can't no more." Using the first letter of each word of these two lines of the song results in a password that looks like this: **yigtmhttotrigrticnm**

Now that you are armed with this handy-dandy tactic, be sure to rinse and repeat with all your passwords so they are different. Please, please do not re-use your passwords, especially on your government issued devices and/or accounts.

Remember, once a cyber criminal gets one of your passwords, they will try it on **all your accounts**. They are lazy, people. Make them work for the goods.

Check out the full Newsweek article here to see the remaining 6 tips to create a unique and strong password every time.

‹ Back to Announcements (b) (6) Search

Cyber Wise Security Tip: Be Aware of Fake COVID-19 Web Content

(b) (6)

Please be advised that hackers and nation-state attackers are capitalizing on the recent COVID-19 pandemic and creating fake websites touting updates and geographic information relating to the spread of COVID-19.

These sites are pretending to show the live map for COVID-19 Global Cases by Johns Hopkins University.

Be careful, the act of visiting the website infects the user with an information-stealing program which can exfiltrate a variety of sensitive data. It is likely being spread via infected email attachments, malicious online advertisements, and social engineering.
Furthermore, anyone searching the internet for a Coronavirus map could unwittingly navigate to this malicious website.
Users should be aware of the risks associated with web content from untrusted sites and only navigate to official sources in the pursuit of information regarding COVID-19.

CISA has a really great resource on their page to keep you up to date on how to keep staying cyber safe with COVID-19, take a look here .

Thanks,
Your Cyber Training Team

❮ Back to Announcements (b) (6) Search

Cyber Wise Tip: Watch out for Bogus COVID-19 Scams

Hi All,

(b) (6)

Unfortunately, there have been a rise in online scams using Corona virus to try and take advantage of people during this time. Last week we posted about attackers using a fake live map from John Hopkins University to infect concerned citizen.
Please be wary and a little skeptical of any unsolicited advice or guidance about the Corona virus. We advise using your best judgement and highly trusted news resources when staying informed.

Two more scams to look out for:

1) World Health Organization (WHO) COVID-19 scam:
Phishing emails sent to users which encourages them to download an attachment by clicking on a link called "Safety measures". PLEASE DO NOT CLICK. The WHO will never email attachments that were not explicitly requested. Visit www.who.int/about/communications/cyber-security to read about cyber tips from WHO.

2) CDC Doctor COVID-19 Scam:

Phishing attacks where emails from fake doctors from the CDC are sent to users promising secret information regarding how to stay protected from COVID-19. These secrets do not exist so please do not click on any links promising this information. Please go directly to the CDC web page, to stay up-to-date on their reporting's. For up-to-date COVID-19 info from the CDC visit www.cdc.gov/coronavirus/2019-ncov/index.html

Remember that cyber criminals often use tactics like sense of urgency to try and trick you to go against your better judgement. Don't reward them for it.
Be sure not to click links you are not sure about (**pro-tip:** hover over the link to see the URL, if it's is not trustworthy don't click).

-Your Cyber Training Team

Back to Announcements (b) (6) Search

Cyber Wise Tip: Don't fall for these Coronavirus online scams

(b) (6)

As we are all working to figure out a way to stay safe and informed as the Coronavirus continues impacting our lives, we will be using our Cyber tips to notify you of online scams (such as malware and ransomware attacks spread through emails and apps) to the best of our ability.

Here are the latest COVID-19 scams you should be aware of:

APT36, an Advanced Persistent Threat group posing as the government of India

There is currently an online attack that pretends to provide corona virus guidance from the Indian government, but is actually a program managed from a remote distance (remote access Trojan) to steal your data.

It's believed that this scam comes from a Pakistani state-backed threat actor. It is designed to look like a coronavirus health advisory, but once a user clicks the link on the attached document the program installs remote access trojans on your device and goes to work discovering your devices specs to pull out your data.

Please look out for emails with links appearing as *(email.gov.in.maildrive [.]email/?att=1579160420)*. If you receive this link please do not click on any links, just forward to our Cyber SOC team via (b) (6)

Many state-sponsored threat actors are in on the fun

Don't believe the stereotype about the guy sitting in his mothers basement as the cyber criminal you should fear.
There are many instances were nations-state actors are bankrolling expansive teams in order to hack our government networks and resources. We know that China, Russia, and North Korea already have the following groups using the coronavirus outbreak to attempt online scams:

- Chinese APT: Vicious Panda, Mustang Panda
- North Korean APTs: Kimsuky
- Russian APTs: Hades group (ties with APT28), TA542

Especially on your Bureau provided devices, please be very aware of who is sending you emails with attachments and links before you open or click.

Stop and think before you click.
By hovering over the link with your mouse and using the attachment preview option, you can see the link or attachment before you act on it.

-Your Cyber Training Team

‹ Back to Announcements

(b) (6)

Search

Cyber Wise Tip: Beware Android ransomware posing as a Coronavirus tracking app

(b) (6)

Please watch out for an android app called **Coronavirus Tracker** from the URL *hxxp://coronavirusapp[.]site/mobile.html* .

Do not download on your personal mobile devices. While it alleges to track the spread of coronavirus globally, the app actually is ransomware meaning it will lock you out of your phone and demand you pay money to unlock it.

It will attempt to trick users into allowing it to have admin access by stating that it will notify you if an infected patient is close to you, but is actually trying to gain admin access to your phone to lock you out and begin the attack.

The app is also persistent, meaning even if you reboot your device the app will execute every time.

Cyber pro-tip: Be very skeptical of any application requesting administrative privileges. It is a huge red flag to watch out for. If an app is asking for admin access, you are essentially giving them the master key to control your device.
Really stop and question if an application should have that much control over your device before granting it.

Luckily this app is not that complicated to remove.
Zscaler has a resource to assist in better understanding how to remove the app here.

If you are a victim of the ransomware, you can use **pin** (b) (6) [redacted] to unlock your device.
Then remove the app from the Apps list on your device, under the Settings feature on your device ASAP.

T&I is assessing the risk similar external apps pose to Bureau-issued iPhones. Please stay tuned for any updates.

-Your Cyber Training Team

(b) (6)

‹ Back to Announcements

Search

Cyber Wise Tip: How to stay Cyber safe at home

(b) (6)

Following our tips on Coronavirus scams to keep an eye out for last week (all tips can be found on our wiki page), we wanted to provide a few tips on how to protect your cybersecurity at home:

- Be sure to only use the CFPB provided teleworking resources for work activities

  CFPB provided resources perfect for working at home securely during this time, such as Cisco Always-on-VPN (always-on-virtual private network), mobile device, laptop, and teleconferencing lines (Skype and/or Webex/Mymeetings).

  It's important to conduct all your work using devices that already have enhanced security features. That will slow down and prevent bad actors from using your account to access government network resources.

- Update your passwords and use Two Factor whenever possible

  On your home network, be sure to update your passwords. Remember to use complex and different passwords for every account you have (email, social media, food delivery accounts, etc).

We also recommend turning on two factor authentication on your personal email accounts as well. Google, Microsoft, and RSA all have account authentication apps you can download to your mobile device from your App store. With that app on your phone, it will send an alert to your phone once someone (hopefully you) enters a password to access your account. This allows you have to permit access to your account two times, before you can actually login.
Imagine how much more difficult that feature will make it for cyber criminals to access your account.

- Be aware of Phishing Scams

It can be easy to let your guard down when working from a more non-traditional work setting, but remember to always *Stop and think, before you click*

Take an extra second and hover on the URL provided to you. Is it from someone you know? Were you expecting this link or resource? If so, proceed as usual.
If you answered no to any of the questions I asked you to ask yourself, try and utilize the preview attachment feature available in your email. That is a feature that allows you to take a look at parts of the attachment without downloading or opening the full attachment.

If you believe this is a potential scam, please forward to our Cyber team via (b) (6)
Use your best judgement when opening emails, especially if it's COVID-19 related.

- Be wary of emails and phone calls asking for COVID-19 donations

Do your research first, especially for organizations unfamiliar to you. If you want to donate, we suggest running a quick verify of the charity's authenticity before making donations.
Check the Federal Trade Commission's website for more information about donating at https://www.consumer.ftc.gov/articles/0074-giving-charity

If the violation occurred on your personal device (non-government issued laptop, cell phone, etc),you can report it to the FTC. To report fraud to the Federal Trade Commission, visit www.ftc.gov/complaint

Check out our Cyber Tip of the week wiki page for our archive full of helpful cybersecurity tips, wiki page

-Your Cyber Training Team

‹ Back to Announcements (b) (6) Search

Cyber Wise Tip: Detect a COVID-19 Phishing scam with these red flags

(b) (6)

We wanted to provide a few tips on the red flags to look out for that might indicate you are being targeted for a Coronavirus scam email.
Cofense has a fun info-graphic that you can view on their website

Use sense of urgency language?
If the sender is someone you are not familiar with and use words that attempt to play on fear or try to rush you, that's a major red flag.
For instance, if they ask you to click a link to learn about *high risk areas* or *infection rates near you now*, they may be trying to get you to act fast.
Remember, **stop and think before you click**. We recommend relying on the World Health Organization, CFPB, and CDC's websites as official sources.

Asking for your info?
Is the person asking for your information?
Think about it, does it make sense for a public health organization or professional that you don't know to ask for your personal information?
If the email is doing so, that is a major red flag.
As we mentioned previously, the FTC has a resource you can access to check if there is a charity you are interested in financially supporting.
Check the Federal Trade Commission's website for more information about donating - https://www.consumer.ftc.gov/articles/0074-giving-charity

Using awkward phrasing?
I know you have gotten emails using *Greetings Sir or Madam*. **Red flag.**
If someone is using extremely generic and unspecific greetings like a stranger, you should probably treat them like a stranger.
Please do not trust an untrusted source. Forward the email to our analysts to review via (b) (6)

Grammar and spelling errors?

You would be surprised, but often phishing emails have spelling or grammar mistakes that a business professional normally wouldn't make. If it doesn't read right, something else is probably not right.

If you believe this is a potential scam, please forward to our Cyber team via (b) (6)

Use your best judgement when opening emails, especially if it's COVID-19 related.

Check out our Cybersecurity tip of the week wiki page for our archive full of helpful cybersecurity tipshere

-Your Cyber Training Team

‹ Back to Announcements (b) (6) Search

Cyber Wise: Staysafeonline.org resources for home online safety

(b) (6)

STOP. THINK. CONNECT.™ is a global online safety awareness campaign to help all digital citizens stay safer and more secure online. The Department of Homeland Security leads the federal side of the campaign with leadership provided by the National Cyber Security Alliance (NCSA). The campaign was launched in October of 2010 in partnership with the U.S. government, including the White House.

Since everyone is online more than usual, we wanted to reference the free online security checkups and tools you may want to check out from STOP. THINK.CONNECT

One of the resources listed is the Cisco tool OpenDNS:

OpenDNS

DNS stands for Domain Naming Service. It's the service that runs when you access the internet to resolve host names (think google.com) to IP addresses ((b) (6) to pull in the web resources that you need to access.

- OpenDNS Web content filtering keeps parents in control of what websites children visit at home.

- OpenDNS blocks phishing websites that try to steal your identity and login information by pretending to be a legitimate website.

Visit https://staysafeonline.org/stay-safe-online/free-online-security-checkups-tools/ for the full list of free resources you may want to implement on your home network.

Check out our Cyber Tip of the week wiki page for our archive full of helpful cybersecurity tips here

-Your Cyber Training Team

‹ Back to Announcements (b) (6) [redacted] Search

Cyber Wise Tip: Beware of stimulus relief fraudulent activities

(b) (6) [redacted]

The Secret Service is observing a rise in stimulus relief fraud over the past several days and expect the fraud attempts to continue throughout the pandemic. Criminal actors are using a variety of means to contact potential victims. In one instance, the criminal actors are using spoofed email addresses posing as U.S. Treasury officials requesting that the victim provide personal identifying information (PII), so that they can receive their share of the stimulus.

Criminal cyber actors are exploiting the COVID-19 pandemic through scams and malicious activity. These actors seek to profit from a sudden growth in teleworking, increased use of virtual education systems for online classes, a surge in online shopping, public appetite for information related to the pandemic, and the criticality of maintaining functioning critical infrastructure networks, particularly in the Healthcare and Public Health Sector. Attackers are attempting to deliver Remote Access Tool (RAT) payloads on the systems of small businesses via phishing emails impersonating the U.S. Small Business Administration (U.S. SBA)

-

US Secret Service (USSS) Field Offices and USSS Electronic Crimes Task Forces around the country are actively working with federal, state and local partners to combat cyber enabled fraud, such as ransomware and business e-mail compromise attacks against the health care industry and state/local governments.

- FEMA has created a Coronavirus Rumor Control page: https://www.fema.gov/Coronavirus-Rumor-Control

- New government website for COVID-19 guidance:

https://www.coronavirus.gov/

(b) (6)

‹ Back to Announcements

Search

Cyber Wise Tip: Malware, explained

(b) (6)

Malware is malicious (purposefully harmful) software. There are many software programs that carry out malicious activities such as viruses, worms, ransomware, rootkits, and logic bombs.

Virus is a malicious code that attaches itself to the host application. Once the host application is executed, the malicious code will execute.

Worm A self-replicating kind of malware that travels through a network. They do not need any user action in order to run.

Ransomware
A kind of malware that is used to extort money from people and/or organizations. Often encrypts your data and demands ransom payment before decrypting the data.

RootkitsMalware that gains system-level access to your computer. Often able to hide themselves from users and antivirus software.

Logic bombs
Malware that executes in response to an event. The event can be a specific date/time, or an action like a user launched program.

The best way to control malware is through prevention.
By not downloading programs or clicking on email attachments from unknown sources in the first place, you will be able to prevent it from getting on your computer.

Remember to always, *stop and think, before clicking*.

-Your Cyber Training Team

(b) (6)

❮ Back to Announcements

Search

Cyber Wise Tip: Botnets, explained

(b) (6)

Botnet is the generic name given to any collection of compromised PCs controlled by an attacker remotely — think "virtual robot army." The individual PCs that are part of a botnet are known as "bots" or "zombies," and their owners may not even know they're being used.

Beware, many botnets are typically designed to harvest data, such as passphrases, Social Security numbers, credit card numbers, addresses, telephone numbers and other personal information. The data is then used for nefarious purposes, such as identity theft, credit card fraud, spamming (sending junk email), website attacks and malware distribution.

(b) (6)

‹ Back to Announcements Search

Cyber Wise Tip: Spyware, explained

(b) (6)

Spyware (also known as adware) is software often installed on a computer system to monitor the computer and end-user's activities without the user's awareness or consent. This often includes collecting confidential data such as passwords, PIN numbers, credit card numbers, monitoring keyword strokes, and tracking browsing habits and harvesting email addresses.

This also tends to affect network performance, slowing down the system and affecting the whole business process. It is generally classified into four main categories: Trojans, adware, tracking cookies and system monitors.

- Trojan spyware that infects computers in the form of Trojan malware.
- Adware that also serves as spyware to monitor computers and devices.
- Tracking cookie are files put on hard drives by website that track a user on the Internet if a site is aware of the tracking cookies and designed to use them.
- System monitors are designed to monitor any activity on a computer and capture sensitive data such as keystrokes, sites visited, emails and more.

The best way to control spyware is by preventing it from getting on your computer in the first place. We know not downloading programs and never clicking on email attachments isn't always an option, so try to remember to always *stop and think, before clicking*

‹ Back to Announcements (b) (6) Search

Cyber Wise Tip: You are always the target

It's important to keep in mind that you, as the end-user, are always the target of a cyber-crime.

(b) (6)

A common user misconception is that their data is not valuable and therefore would not be the target of an attack. This assumption is incorrect -- all personal, government, or corporate information is valuable to the right buyer, and any user with an online presence can be a target.

While some risk is inherent with any online activity, it's important to know that everyone has a key role to play in cyber safety whether onsite or at home.

For more actionable tips on how to stay Cyber Wise, check out our Cybersecurity Tip of the week archive at

(b) (6)

(b) (6)

‹ Back to Announcements Search

Cyber Wise Tip: Bluesnarfing, explained

(b) (6)

There are many ways which your Bluetooth-enabled device can be compromised. One way is with bluesnarfing via which a cyber-criminal steals your information by using a Bluetooth connection to hack into your phone.

Many mobile capabilities, including Airdrop, use Bluetooth LE to broadcast and discover connections and point-to-point Wi-Fi to transfer data. While these attacks are rare and require close physical proximity, leaving these Airdrop features enables increases the risk an attacker will find and target your mobile device.

Check to see if your device allows for PIN numbers or passwords to be used for your Bluetooth enabled devices when pairing or turn off your Bluetooth when not in use. When in public places be wary of accepting unexpected connection requests – including unsolicited airdrops.

For more actionable tips on how to stay Cyber Wise, our wiki page offers tips on Mobile Device security 101 and what you should know about mobile app security

Check out our full archive of security tips on our Cyber wiki page -
(b) (6)

-Your Cyber Training Team

(b) (6)

‹ Back to Announcements

Search

Cyber Wise Tip: Advanced Persistent Threats (APT)

(b) (6)

Advanced persistent threat (APT) style cyber-attacks usually involve politically or financially-motivated actors with the skills and intention of deploying a targeted and sophisticated attack on a single entity.

With the evolving global health situation, APT style attacks are on the rise as nation states or enterprising cyber criminals attempt to exploit user vulnerabilities.

The best action is prevention.

Remember to always stay vigilant and on alert for potential suspicious activity.
Be sure to check out the social engineering tactics we've previously mentioned available on our Tip of the week wiki page

-Your Cyber Training Team

‹ Back to Announcements (b) (6) Search

Cyber Wise Tip- Here's why you probably shouldn't share your old senior photos on Facebook

(b) (6)

In a recent social media trend, people have been sharing their own senior photos on Facebook with the hashtag #ClassOf2020. This is meant to be an act of solidarity with students who have had their graduation ceremonies cancelled due to COVID-19.

However, these posts could help potential hackers crack into your private accounts.

Attackers scan sites like Facebook for this hashtag where they can also find the name of a person's high school and graduating year -- two common online security questions. And if that user's social media account is not set to private, hackers can find plenty of data that they can use for social engineering attacks.

Before sharing, users should make sure their accounts are set to private and that they are using strong passwords for all accounts. Also, ensure there is no public-facing information on social media sites that users would not like in the hands of a hacker.

(b) (6)

‹ Back to Announcements Search

Cyber Wise Tip- Email attachments, click with caution

Did you know email attachments are often used as tools for attacks by cyber criminals?

(b) (6)

Think about how easy it is to circulate messages to thousands, even millions of people with just a few clicks. Many of the programs we use day-to-day offer the ability to download attachments automatically, which can lead to an unsuspecting user downloading a virus without a second thought.

<u>Tips to keep yourself protected:</u>

- Be wary of unsolicited attachments, even from people you know. Many viruses can "spoof" the return address, making it look like the message came from someone else.

- Keep software up to date. Always comply with CFPB prompts for system updates in a timely manner

‹ Back to Announcements (b) (6) Search

Cyber Wise Tip- Denial-of-Service Attacks, explained

(b) (6)

A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. This may impact services including email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network.

A denial-of-service attack is accomplished by flooding the targeted website or service with traffic until the target cannot respond or simply crashes, preventing access for legitimate users

Symptoms of an attack include unusually slow network performance (opening files or accessing websites), unavailability to access an individual website or any websites. If you believe a system has been the target of such an attack, there are a few recommended steps to take.

On the CFPB network:
If you are connected to the internet but are losing connection to any Bureau systems, contact the CFPB Service Desk (b) (6)) to report the issue and get advised on the appropriate steps to take.

On a home network:
Check to see if other devices in your home are connected. If multiple devices lost connection, you can reach out to your Internet Service Provider (ISP) to ask if there is an outage on their end and they will advise you on an appropriate course of action.

(b) (6)

‹ Back to Announcements

Search

Cyber Wise Tip- Beware of COVID-19 Email Phishing Against US Healthcare Providers

(b) (6)

Following a global increase in malicious cyber activity exploiting the uncertainties from the COVID-19 pandemic, the FBI was notified of targeted email phishing attempts against US-based medical providers.

These attempts use COVID-19 related email subject lines and content to distribute malicious attachments, which exploited Microsoft Word Document files, 7-zip (.7z) compressed files, Microsoft Visual Basic Script, Java, and Microsoft Executables.

Here are a few examples of some of the known characteristics of the scam message:

Email Subject:	**Attachment Filename:**
PURCHASE ORDER PVT	Doc35 Covid Business Form.doc
Returned mail:see transcript for details	Covid-19_UPDATE_PDF.7z
COVID-19 UPDATE !!	Covid-19_UPDATE_PDF.7z
Information about COVID-19 in the United States	covid50_form.vbs

Steps to take to stay CyberWise:

-Be wary of unsolicited attachments, even from people you know. Cyber actors can "spoof" the return address, making it look like the message came from a trusted associate.
-Keep software up to date. Install software patches when prompted so that attackers can't take advantage of known vulnerabilities.
- If an email or attachment seems suspicious, don't open it, even if your antivirus software indicates that the message is clean. Attackers are constantly releasing new viruses, and the antivirus software might not have the signature.
-If possible, turn off the option to automatically download attachments. Check your email settings to see if your software offers the option and disable it.

If you believe you are being targeted by a phishing campaign, please do not open the attachment – just forward it to our Cyber Operations team via (b) (6) [redacted] or use the Report Phishing button available in your CFPB Outlook application.

-Your Cyber Training Team

(b) (6)

‹ Back to Announcements

Search

Cyber Wise Tip: Watch out for spoofed emails!

(b) (6)

We have seen an increase in attacks recently since bad actors often increase the frequency and severity of cyber-attacks during the current global heal crisis. One attack that is particularly popular with hackers lately is sending phishing email attacks to your work email that appear to come from your supervisor/boss. We experienced one of these attacks just today, with an attempt that appeared to come from the Director.

A bad actor can pose as top level officials by masquerading their "From" email address, a signature or weblinks. Federal email addresses, like the ones we use at CFPB, can be requested via a Freedom of Information Act (FOIA) request. Some scammers may even send a spam email to your boss first to see if it is auto-replied with an "out of office" message, specifically so they can reach out to you under your boss' names since they are not in the office.

The boss gift card scam is so simple and requires almost no tech know-how. The email claims to be from your boss or someone you know. They might have "spoofed" your boss' work email by subtly changing the address (e.g. John.Doe@cfpb.net), actively hacked into someone's account, or are pretending they are locked out of their account and using a stranger's phone or computer.

In this email scam, you are given a very plausible story as to why they need you to click on a link or send them something. These emails might ask you to buy a gift card and send over the numbers from the back or ask you to open a malicious attachment.

It is important to remember that there is no plausible reason why someone at work would need you to purchase a gift card. Most major companies will sell their gift cards in stores and online, and retailers like Amazon and Walmart who sell other companies' gift cards will even sell others' cards on their websites. The best way to avoid becoming a victim of this type of attack is to report emails to the security operations center ((b) (6) [redacted]) and refrain from clicking all links or replying. Trust your instincts and protect yourself (and the organization).

If you suspect you have received a malicious email from a spoofed email address, report it using the "report phishing" button in your outlook or forward as an attachment to (b) (6) [redacted]. For additional questions or information, please reach out to the Cybersecurity Training Team at (b) (6) [redacted]

-Your Cyber Training Team

(b) (6)

‹ Back to Announcements

Search

Cyber Wise Tip: Watch out for Spear Phishing & Whaling Attacks

(b) (6)

A highly targeted form of phishing, spear phishing involves hackers sending tailored and personal emails to well-researched victims purporting to be a trusted sender. Spear phishing attacks are hard to spot without close inspection and difficult to stop with technical controls alone. While regular phishing campaigns go after large numbers of relatively low-yield targets, spear phishing aims at specific targets using specially emails crafted to their intended victim.

Some targeted spear phishing attacks involve documents containing malware or links to malicious web sites to steal sensitive information or valuable intellectual property, or to simply compromise payment systems.

(b) (5)

Spear-phishing attacks targeting high-level executives are often known as whale phishing attacks, and usually involve an attacker attempting to impersonate the CEO or similarly important person within the organization with the aim of using superiority to coerce the victim into sharing information.

How to spot & thwart a spear phishing attack

The Bureau employs many technical controls to prevent spear phishing emails from reaching your inbox including spam filters, malware detection and antivirus. However these controls will not stop 100% of targeted attacks. Here are some characteristics of these types of attacks and actions for preventing them:

-Examine the actual email address to ensure it is from CFPB. While the email sender alias might appear to be the name of your supervisor or other high-profile CFPB individual, the email address itself will often not be a CFPB Email Address

- Watch out for vague language or a generic request to click on a link or enter information.

-Call the individual personally if possible to see if the message was legitimate

If you believe a message is suspicious, report it using the "report phishing" button in outlook or by sending as an attachment to(b) (6) [redacted]

Bureau of Consumer Financial Protection
1700 G Street NW
Washington, D.C. 20552

March 20, 2020

The Honorable Patrick McHenry
Ranking Member
Committee on Financial Services
U.S. House of Representatives
4340 O'Neill House Office Building
Washington, D.C. 20024

Dear Ranking Member McHenry:

Thank you for your letter dated March 16, 2020, concerning the Consumer Financial Protection Bureau's (Bureau's) efforts to assist customers, especially older Americans, and communities affected by the Coronavirus Disease 2019 (referred to as COVID-19). As you know, this is an evolving situation; as such we are continually monitoring and responding to new developments.

Thank you for your recommendation to update existing interagency guidance on financial abuse of older adults. The Bureau continues to stand behind the 2013 Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults, and the Bureau and its interagency partners have been working to provide further guidance to financial institutions in response to concerns raised by COVID-19. As you know, on March 6, 2020, the Federal Financial Institutions Examination Council (FFIEC) issued updated guidance titled Interagency Statement on Pandemic Planning.[1] This guidance identifies actions that financial institutions should take to minimize the potential adverse effects of a pandemic. In addition, on March 9,

[1] https://www.ffiec.gov/press/PDF/FFIEC%20Statement%20on%20Pandemic%20Planning.pdf.

2020, the Bureau, with its interagency partners, issued a press release, encouraging financial institutions to work constructively with borrowers and other customers affected by COVID-19. Many financial institutions want to help customers navigate this situation. We recommend that consumers contact their financial institutions to discuss their specific circumstances. We have also reiterated that the Bureau stands ready to help consumers resolve issues with their financial services providers who submit a complaint through our consumer complaint system. The Bureau will take your recommendation for additional guidance into account as we continue to monitor and assess the current situation.

On March 18, 2020, I issued a statement after the U.S. Department of Housing and Urban Development (HUD) and the Federal Housing Finance Agency (FHFA) announced a moratorium on foreclosures and evictions.[2] In my statement, I noted that the actions taken by HUD and FHFA are timely and an important step in providing assurance to consumers. I commend my colleagues at HUD and FHFA for being proactive on this issue and providing Americans with much needed peace of mind during this uncertain time.

This week, the Bureau launched a dedicated page on our website for all COVID-19 resources to help consumers protect themselves financially from the impact of COVID-19.[3] As consumers plan for the potential impact of COVID-19, there are a number of steps they can take to help themselves or a loved one financially, both in the short and long term. The Bureau's initial blog post, posted on March 16, 2020, includes information for steps to take in the following situations: (1) if consumers have trouble paying their bills or meeting other financial obligations; (2) if consumers experience a loss of income; and (3) if consumers think they may be targeted by a scammer.[4] On March 17, 2020, the Bureau posted additional resources to help consumers make informed financial decisions with up-to-date information and resources, including information on how consumers can submit complaints to the Bureau if they are

[2] https://www.consumerfinance.gov/about-us/newsroom/cfpb-director-kraninger-statement-joint-hud-fhfa-announcement-foreclosure-and-eviction-moratorium/.

[3] https://www.consumerfinance.gov/coronavirus/.

[4] https://www.consumerfinance.gov/about-us/blog/protect-yourself-financially-from-impact-of-coronavirus/.

having a problem with a financial product or service.[5] The Bureau's website can also help consumers with resources to prepare and recover from emergencies, be they natural disasters or pandemic events. Our team is ready to help consumers resolve issues with their financial services providers who submit a complaint through our consumer complaint system.

As you noted, scammers often target older adults. As older adults are at a higher risk for serious illness they may also be isolating themselves.[6] Social isolation is already an issue for older adults and can lead to a host of issues, including an increased likelihood of falling for scams due to a need to connect to others. This issue could grow in response to virus prevention tactics like social distancing and quarantines. The Bureau's Money Smart for Older Adults Resource guide,[7] which is designed to help older adults, family caregivers and others prevent, recognize, and report financial exploitation, and the Protecting Residents from Financial Exploitation guide,[8] which is designed to help assisted living and nursing facility managers and staff prevent and address elder financial exploitation of their residents, also may be helpful.

As the Bureau continues to assess and evaluate the situation surrounding COVID-19, the health and safety of our staff continues to be my top priority. Although the Bureau's supervisory activities and other essential functions involving financial institutions will continue, unless otherwise directed, Bureau examination activity of Bureau-supervised institutions will be conducted off-site, from examiners' home duty stations, for two weeks starting Monday, March 16 through Friday, April 3. The Bureau also has implemented a mandatory telework policy for all Bureau employees with a telework agreement. This mandatory telework began on Monday, March 16 for employees who work at 1700 G St. and the New York Regional Office, and was applied to all Bureau employees on March 18. This will continue through Friday, April 3. In addition, the Bureau Headquarters and the New York Regional Office have been deep cleaned and access to the buildings is restricted; other regional offices have enhanced their cleaning

[5] https://www.consumerfinance.gov/about-us/blog/cfpb-helps-consumers-make-informed-financial-decisions-with-up-to-date-information-and-resources/.

[6] https://www.cdc.gov/coronavirus/2019-ncov/specific-groups/high-risk-complications.html.

[7] https://www.consumerfinance.gov/practitioner-resources/resources-for-older-adults/protecting-against-fraud/.

[8] https://files.consumerfinance.gov/f/201406_cfpb_guide_protecting-residents-from-financial-exploitation.pdf

procedures, too. These steps are intended to promote the well-being of our workforce so they can ensure the delivery of our important mission.

The Bureau is continuing to monitor the impact of COVID-19 and will issue additional information and guidance, as warranted. Should you have any questions, please do not hesitate to contact me or have your staff contact Kate Fink in the Bureau's Office of Legislative Affairs. Ms. Fink can be reached at (b) (6)

Sincerely,

Kathleen L Kraninger

Kathleen L. Kraninger
Director

cc: The Honorable Ann Wager, Vice Ranking Member, Committee on Financial Services
The Honorable Bill Huizenga, Ranking Member, Subcommittee on Investor Protection, Entrepreneurship, and Capital Markets
The Honorable French Hill, Ranking Member, Subcommittee on National Security, International Development, and Monetary Policy
The Honorable Blaine Luetkemeyer, Ranking Member, Subcommittee on Consumer Protection and Financial Institutions
The Honorable Andy Barr, Ranking Member, Subcommittee on Oversight and Investigations
The Honorable Steve Stivers, Subcommittee on Housing, Community Development, and Insurance

Bureau of Consumer Financial Protection
1700 G Street NW
Washington, D.C. 20552

March 20, 2020

The Honorable Mark R. Warner
United States Senate
703 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Sherrod Brown
United States Senate
534 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senator Warner and Senator Brown:

Thank you for your letter dated March 9, 2020, concerning the Consumer Financial Protection Bureau's (Bureau's) efforts to provide financial institutions with guidance to help assist customers and communities affected by the Coronavirus Disease 2019 (referred to as COVID-19) in a manner that is consistent with safe and sound banking practices. The Bureau appreciates this opportunity to update you on the status of the actions taken to-date to provide guidance to the financial industry in response to concerns raised by COVID-19. As you know, this is an evolving situation; as such we are continually monitoring and responding to new developments.

On March 6, 2020, the Federal Financial Institutions Examination Council (FFIEC) issued updated guidance titled Interagency Statement on Pandemic Planning.[1] This guidance identifies actions that financial institutions should take to minimize the potential adverse effects of a pandemic. Specifically, a financial institution's business continuity plan should address pandemics and provide a documented strategy scaled to the stages of a pandemic outbreak that is sufficiently flexible to address a wide range of possible effects that could result from a

[1] https://www.ffiec.gov/press/PDF/FFIEC%20Statement%20on%20Pandemic%20Planning.pdf.

pandemic and is appropriate for the financial institution's size, complexity, and business activities. The guidance recognizes that sound planning in advance of any imminent risk helps to minimize a disruption in services to consumers, businesses, and communities when such contingencies occur.

In addition, on March 9, 2020, the Bureau, with its interagency partners issued a press release, encouraging financial institutions to work constructively with borrowers and other customers affected by COVID-19. The Bureau has existing regulatory flexibility in our mortgage servicing rules that should make it easier for mortgage servicers to quickly offer short-term help (such as forbearance) to homeowners who may start to have trouble making their mortgage payments.[2] We know consumers' first stop in the face of hardship is with their creditors and their financial institutions, so our message was important for regulated entities to hear. We also know many financial institutions want to help customers navigate this situation. I will continue to work with our Federal and State partners, and seek feedback from stakeholders, to ensure we are providing appropriate flexibilities to benefit consumers during this time.

On March 18, 2020, I issued a statement after the U.S. Department of Housing and Urban Development (HUD) and the Federal Housing Finance Agency (FHFA) announced a moratorium on foreclosures and evictions.[3] In my statement, I noted that the actions taken by HUD and FHFA are timely and an important step in providing assurance to consumers. I commend my colleagues at HUD and FHFA for being proactive on this issue and providing Americans with much needed peace of mind during this uncertain time.

This week, the Bureau launched a dedicated page on our website for all COVID-19 resources to help consumers protect themselves financially from the impact of COVID-19.[4] As consumers plan for the potential impact of COVID-19, there are a number of steps they can take to help

[2] https://www.consumerfinance.gov/policy-compliance/guidance/supervisory-guidance/statement-supervisory-practices-regarding-financial-institutions-and-consumers-affected-major-disaster-or-emergency/.

[3] https://www.consumerfinance.gov/about-us/newsroom/cfpb-director-kraninger-statement-joint-hud-fhfa-announcement-foreclosure-and-eviction-moratorium/.

[4] https://www.consumerfinance.gov/coronavirus/.

themselves or a loved one financially, both in the short and long term. The Bureau's initial blog post, posted on March 16, 2020, includes information for steps to take in the following situations: (1) if consumers have trouble paying their bills or meeting other financial obligations; (2) if consumers experience a loss of income; and (3) if consumers think they may be targeted by a scammer.[5] On March 17, 2020, the Bureau posted additional resources to help consumers make informed financial decisions with up-to-date information and resources, including information on how consumers can submit complaints to the Bureau if they are having a problem with a financial product or service.[6] The Bureau's website can also help consumers with resources to prepare and recover from emergencies, be they natural disasters or pandemic events. Our team is ready to help consumers resolve issues with their financial services providers who submit a complaint through our consumer complaint system.

As the Bureau continues to assess and evaluate the situation surrounding COVID-19, the health and safety of our staff continues to be my top priority. Although the Bureau's supervisory activities and other essential functions involving financial institutions will continue, unless otherwise directed, Bureau examination activity of Bureau-supervised institutions will be conducted off-site, from examiners' home duty stations, for two weeks starting Monday, March 16 through Friday, April 3. The Bureau also has implemented a mandatory telework policy for all Bureau employees with a telework agreement. This mandatory telework began on Monday, March 16 for employees who work at 1700 G St. and the New York Regional Office, and was applied to all Bureau employees on March 18. This will continue through Friday, April 3. In addition, the Bureau Headquarters and the New York Regional Office have been deep cleaned and access to the buildings is restricted; other regional offices have enhanced their cleaning procedures, too. These steps are intended to promote the well-being of our workforce so they can ensure the delivery of our important mission.

[5] https://www.consumerfinance.gov/about-us/blog/protect-yourself-financially-from-impact-of-coronavirus/.

[6] https://www.consumerfinance.gov/about-us/blog/cfpb-helps-consumers-make-informed-financial-decisions-with-up-to-date-information-and-resources/.

The Bureau is continuing to monitor the impact of COVID-19 and will issue additional information and guidance, as warranted. Should you have any questions, please do not hesitate to contact me or have your staff contact Kate Fink in the Bureau's Office of Legislative Affairs. Ms. Fink can be reached at (b) (6)

Sincerely,

Kathleen L Kraninger

Kathleen L. Kraninger
Director

cc: The Honorable Robert Menendez, United States Senator
The Honorable Elizabeth Warren, United States Senator
The Honorable Brian Schatz, United States Senator
The Honorable Chris Van Hollen, United States Senator
The Honorable Catherine Cortez Masto, United States Senator
The Honorable Doug Jones, United States Senator

Bureau of Consumer Financial Protection
1700 G Street NW
Washington, D.C. 20552

March 20, 2020

The Honorable Maxine Waters
Chairwoman
Committee on Financial Services
U.S. House of Representatives
2129 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairwoman Waters:

Thank you for your letter dated March 11, 2020, concerning the Consumer Financial Protection Bureau's (Bureau's) efforts to assist consumers, financial institutions, and communities affected by the Coronavirus Disease 2019 (referred to as COVID-19). The Bureau appreciates this opportunity to update you on the status of the actions taken to-date to assist consumers, provide guidance to the financial industry, and protect the Bureau's workforce and facilities in response to concerns raised by COVID-19. As you know, this is an evolving situation; as such we are continually monitoring and responding to new developments.

On March 6, 2020, the Federal Financial Institutions Examination Council (FFIEC) issued updated guidance titled Interagency Statement on Pandemic Planning.[1] This guidance identifies actions that financial institutions should take to minimize the potential adverse effects of a pandemic. Specifically, a financial institution's business continuity plan should address pandemics and provide a documented strategy scaled to the stages of a pandemic outbreak that

[1] https://www.ffiec.gov/press/PDF/FFIEC%20Statement%20on%20Pandemic%20Planning.pdf.

is sufficiently flexible to address a wide range of possible effects that could result from a pandemic and is appropriate for the financial institution's size, complexity, and business activities. The guidance recognizes that sound planning in advance of any imminent risk helps to minimize a disruption in services to consumers, businesses, and communities when such contingencies occur.

In addition, on March 9, 2020, the Bureau, with its interagency partners issued a press release, encouraging financial institutions to work constructively with borrowers and other customers affected by COVID-19. The Bureau has existing regulatory flexibility in our mortgage servicing rules that should make it easier for mortgage servicers to quickly offer short-term help (such as forbearance) to homeowners who may start to have trouble making their mortgage payments.[2] We know consumers' first stop in the face of hardship is with their creditors and their financial institutions, so our message was important for regulated entities to hear. We also know many financial institutions want to help customers navigate this situation. I will continue to work with our Federal and State partners, and seek feedback from stakeholders, to ensure we are providing appropriate flexibilities to benefit consumers during this time.

On March 18, 2020, I issued a statement after the U.S. Department of Housing and Urban Development (HUD) and the Federal Housing Finance Agency (FHFA) announced a moratorium on foreclosures and evictions.[3] In my statement, I noted that the actions taken by HUD and FHFA are timely and an important step in providing assurance to consumers. I commend my colleagues at HUD and FHFA for being proactive on this issue and providing Americans with much needed peace of mind during this uncertain time.

This week, the Bureau launched a dedicated page on our website for all COVID-19 resources to help consumers protect themselves financially from the impact of COVID-19.[4] As consumers

[2] https://www.consumerfinance.gov/policy-compliance/guidance/supervisory-guidance/statement-supervisory-practices-regarding-financial-institutions-and-consumers-affected-major-disaster-or-emergency/.

[3] https://www.consumerfinance.gov/about-us/newsroom/cfpb-director-kraninger-statement-joint-hud-fhfa-announcement-foreclosure-and-eviction-moratorium/.

[4] https://www.consumerfinance.gov/coronavirus/.

plan for the potential impact of COVID-19, there are a number of steps they can take to help themselves or a loved one financially, both in the short and long term. The Bureau's initial blog post, posted on March 16, 2020, includes information for steps to take in the following situations: (1) if consumers have trouble paying their bills or meeting other financial obligations; (2) if consumers experience a loss of income; and (3) if consumers think they may be targeted by a scammer.[5] On March 17, 2020, the Bureau posted additional resources to help consumers make informed financial decisions with up-to-date information and resources, including information on how consumers can submit complaints to the Bureau if they are having a problem with a financial product or service.[6] The Bureau's website can also help consumers with resources to prepare and recover from emergencies, be they natural disasters or pandemic events. Our team is ready to help consumers resolve issues with their financial services providers who submit a complaint through our consumer complaint system.

As the Bureau continues to assess and evaluate the situation surrounding COVID-19, the health and safety of our staff continues to be my top priority. Although the Bureau's supervisory activities and other essential functions involving financial institutions will continue, unless otherwise directed, Bureau examination activity of Bureau-supervised institutions will be conducted off-site, from examiners' home duty stations, for two weeks starting Monday, March 16 through Friday, April 3. The Bureau also has implemented a mandatory telework policy for all Bureau employees with a telework agreement. This mandatory telework began on Monday, March 16 for employees who work at 1700 G St. and the New York Regional Office, and was applied to all Bureau employees on March 18. This will continue through Friday, April 3. In addition, the Bureau Headquarters and the New York Regional Office have been deep cleaned and access to the buildings is restricted; other regional offices have enhanced their cleaning procedures, too. These steps are intended to promote the well-being of our workforce so they can ensure the delivery of our important mission.

The Bureau is continuing to monitor the impact of COVID-19 and will issue additional information and guidance, as warranted. Should you have any questions, please do not hesitate

[5] https://www.consumerfinance.gov/about-us/blog/protect-yourself-financially-from-impact-of-coronavirus/.

[6] https://www.consumerfinance.gov/about-us/blog/cfpb-helps-consumers-make-informed-financial-decisions-with-up-to-date-information-and-resources/.

to contact me or have your staff contact Kate Fink in the Bureau's Office of Legislative Affairs. Ms. Fink can be reached at (b) (6)

Sincerely,

Kathleen L Kraninger

Kathleen L. Kraninger
Director

cc: The Honorable Brad Sherman, Chairman, Subcommittee on Investor Protection, Entrepreneurship, and Capital Markets
The Honorable Gregory W. Meeks, Chairman, Subcommittee on Consumer Protection and Financial Institutions
The Honorable Wm. Lacy Clay, Chairman, Subcommittee on Housing, Community Development, and Insurance
The Honorable Emanuel Cleaver, Chairman, Subcommittee on National Security, International Development and Monetary Policy
The Honorable Al Green, Chairman, Subcommittee on Oversight and Investigations
The Honorable Joyce Beatty, Chair, Subcommittee on Diversity and Inclusion
The Honorable Bill Foster, Chairman, Task Force on Artificial Intelligence
The Honorable Stephen Lynch, Chairman, Task Force on Financial Technology

Bureau of Consumer Financial Protection
1700 G Street NW
Washington, D.C. 20552

April 9, 2020

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing, and
Urban Affairs
United States Senate
534 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Brian Schatz
United States Senate
722 Hart Senate Office Building
Washington, D.C. 20510

Dear Ranking Member Brown and Senator Schatz,

Thank you for your letter dated April 7, 2020, concerning the Consumer Financial Protection Bureau's (Bureau's) efforts to assist consumers, communities, and financial institutions affected by COVID-19. In these extraordinary times, the Bureau remains committed to carrying out its statutory mission and continues to use the tools Congress gave us – education, regulation, supervision, and enforcement – to protect consumers in the financial services marketplace. I know we share this commitment to protecting consumers, so I appreciate the opportunity to update you on our recent actions to prevent financial harm, help families who are struggling financially, and provide guidance to the financial industry to ensure their resources are aimed at assisting consumers in need. Consumers are at the heart of everything we do. As such, I ask for your assistance in getting the word out to your constituents about the Bureau, through consumerfinance.gov, as a resource for accurate, timely, and trusted information.

First and foremost, let me speak to the Bureau's efforts to provide consumers with good information to protect their financial well-being during this period of uncertainty. The imperative for social distancing and other public health mitigation steps have further isolated many Americans in need. It is therefore essential for us to support each other and the most vulnerable among us. Good information is key to that effort, and the Bureau has built upon its excellent basis of materials and capabilities to meet that need.

From the start of the crisis, the Bureau worked quickly to produce and distribute valuable resources for consumers to both understand the potential financial risks posed by the pandemic and manage those risks. On March 13, 2020, the Bureau published the blog post "Protect yourself financially from the impact of the coronavirus"[1] and soon added a Spanish translation of the information[2] as well as a central COVID-19 landing page for consumers.[3] The Bureau has also released resources for consumers with questions about student loan payments,[4] scams,[5] debt collection,[6] and credit scores,[7] among other things. These resources help consumers make informed financial decisions, and the Bureau will continue to update these resources with new information, formats and content as they become available.

You will be happy to know that the production of new content is already being informed by our internal research and consumer complaints teams, as you suggested. For instance, as the economic harm from the virus spread, the Bureau began receiving an increase in consumer inquiries about mortgage products. In response, the Bureau released a guide for borrowers on the options available to them, including requesting forbearance under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act),[8] and a video explanation[9] of the mortgage programs in the CARES Act. So far, the Bureau's materials have been viewed over 500,000 times, and we are working with partners such as Google to make sure that the consumers most in need of our resources are able to find them. Additionally, understanding that older Americans may be most vulnerable to the virus and therefore least able to visit a physical bank at this time, the Bureau published a guide for consumers new to online banking that explained how to safely access these services for the first time.[10]

While most Americans can be counted upon to pull together and support one another during this crisis, the Bureau is aware that bad actors will seek to take advantage of vulnerable individuals to perpetrate fraud and scams. Recently, I discussed how to counter their illegal activity and mitigate the impacts on consumers. The Bureau is including information related to

[1] https://www.consumerfinance.gov/about-us/blog/protect-yourself-financially-from-impact-of-coronavirus/.

[2] https://www.consumerfinance.gov/about-us/blog/proteja-sus-finanzas-del-impacto-del-coronavirus/.

[3] https://www.consumerfinance.gov/coronavirus/.

[4] https://www.consumerfinance.gov/about-us/blog/what-you-need-to-know-about-student-loans-and-coronavirus-pandemic/; https://www.consumerfinance.gov/about-us/blog/prestamos-estudiantiles-y-coronavirus/.

[5] https://www.consumerfinance.gov/about-us/blog/beware-coronavirus-related-scams/; https://www.consumerfinance.gov/about-us/blog/estafas-relacionadas-con-coronavirus/;https://www.consumerfinance.gov/about-us/blog/avoid-scams-find-help-during-quarantine/.

[6] https://www.consumerfinance.gov/about-us/blog/coronavirus-and-dealing-debt-tips-help-ease-impact/; https://www.consumerfinance.gov/about-us/blog/lidiando-con--coronavirus-y-deudas-consejos-para-aliviar-impacto/.

[7] https://www.consumerfinance.gov/about-us/blog/protecting-your-credit-during-coronavirus-pandemic/; https://www.consumerfinance.gov/about-us/blog/proteja-su-credito-durante-la-pandemia-del-coronavirus/.

[8] https://www.consumerfinance.gov/about-us/blog/guide-coronavirus-mortgage-relief-options/.

[9] https://www.youtube.com/watch?v=br5EPugsnLs.

[10] https://www.consumerfinance.gov/about-us/blog/online-mobile-banking-tips-beginners/.

these scams on our website. The Bureau's Office of Enforcement is closely monitoring the market for signs of illegal consumer financial activity, and I have personally engaged many of our partners in the past few weeks on this topic and will continue to do so. We will act swiftly to counter these scams and enforce the law to the fullest to protect consumers.

Despite the nationwide disruptions being caused by COVID-19, we continue our daily work to help consumers. The Bureau continues its mission of handling consumer complaints. Since our inception, we've built a robust and technologically forward complaint process that handles approximately 30,000 complaints every month. Even in these challenging times, we are sending complaints to companies to help consumers get the response they need. We have also reminded consumers that that the complaint system is a key resource and backstop for them in the current crisis – and one that we use rigorously to inform our work. In addition, the Bureau continues to perform examinations and other supervisory work, albeit remotely for the time being. Our examiners are conducting supervisory activities from their home-duty stations by leveraging technology and adjusting work as necessary. As you know, this is an evolving situation; as such we are continually monitoring and responding to new developments. We will continue to coordinate with all stakeholders in order to take necessary actions to protect consumers and to combat fraud, deception, and abuse.

The Bureau also helps consumers by providing clear rules of the road for those who your constituents interact with in the financial sector; this effort is also important for consumer protection. The Bureau has taken additional steps to protect consumers during the COVID-19 pandemic, including guidance related to the CARES Act. As you know, the CARES Act allows borrowers with a federally-backed mortgage loan to request forbearance from their mortgage servicer if they experience financial hardship due to the COVID-19 pandemic. As you pointed out, mortgage servicers are dealing with "the burden of extremely high call volume," which could inhibit some borrowers from quickly and easily obtaining mortgage forbearance.

On April 3, 2020, the Bureau made clear that the CARES Act forbearance program is a short-term, loss mitigation program under the mortgage servicing rule and, as such, certain consumer protections apply. At the same time, there are notice timelines within the rule that could pose a challenge to responsible financial institutions with staffing shortfalls due to COVID-19 and thus impede their ability to help borrowers get the immediate mortgage relief they need. Further, given many of the consumers are seeking short-term forbearance at this time rather than refinancing or long-term loss mitigation options, the required notices may confuse consumers. As a result, the Bureau reiterated flexibility that mortgage servicers currently have under the rule to alter language in those notices and to delay information regarding long-term loss mitigation options to later in the forbearance period. In addition, the Bureau clarified that it does not intend to take supervisory or enforcement action against a mortgage servicer for delays in engaging in certain loss mitigation procedures, particularly in outlining long-term loss mitigation options where consumers are anticipating only needing short-term forbearance, provided that servicers are making a good faith effort to do so within a reasonable time.[11] This guidance should facilitate mortgage servicers' ability to place borrowers in short-term forbearance quickly, and it responds directly to the challenges of COVID-19 and the programs Congress created in the CARES Act.

Additionally, in response to enactment of the CARES Act, on April 1, 2020, the Bureau informed credit bureaus and lenders that they must comply with the CARES Act.[12] We also provided flexibility for lenders and credit bureaus in the time they take to investigate credit disputes. As we are all experiencing leading our respective organizations during this unprecedented period, the threat of the COVID-19 pandemic has disrupted normal operations and imposed staffing and resource constraints on many organizations, credit bureaus included. The Bureau's flexibility, provided in response to the extraordinary circumstances, ensures that consumers can continue to benefit from an effective, agile consumer reporting industry.

Over the past several weeks, the Bureau has actively engaged with regulated entities, consumer advocates, State partners, and other stakeholders to ensure we are providing appropriate flexibilities to benefit consumers during this time. In your letter, you note the Bureau postponing some data collections from industry. The most notable announcement was postponement of compliance with a new requirement that starting in May 2020, certain financial institutions would need to begin providing Home Mortgage Disclosure Act (HMDA) data quarterly in addition to the annual basis that is now well-established. This temporary and targeted regulatory flexibility is to allow companies to focus on responding to consumers in need. We recognize that many institutions are facing operational challenges due to COVID-19, and the priority must be responding to consumers facing nearer term issues – for example, updating their systems to intake CARES Act forbearance information from customers rather than reporting HMDA data more frequently. As such, we will continue to provide relief as needed to ensure that resources can be focused on consumers.

In this uncertain time, trusted, authoritative government sources are critical conduits for the distribution of information to the public. Let me close by taking this opportunity to ask you personally: please help us get the word out. Share our resources with your constituents. Link our blog posts and videos on your social media accounts and in your newsletters. Direct the people you represent to consumerfinance.gov when answering questions on your virtual town halls. If you are asked questions that are not covered on consumerfinance.gov, I want to know

[11] https://www.consumerfinance.gov/about-us/newsroom/federal-agencies-encourage-mortgage-servicers-work-struggling-homeowners-affected-covid-19/

[12] https://www.consumerfinance.gov/about-us/newsroom/cfpb-issues-credit-reporting-guidance-during-covid-19-pandemic/

about it and we will update our information. Additionally, if you identify opportunities to work together to protect consumers, I am available to you.

Thank you again for your continued engagement with the Bureau's work. Should you have any additional questions, please do not hesitate to contact me, or have your staff contact Kate Fink in the Bureau's Office of Legislative Affairs. Ms. Fink can be reached at (b) (6)

Sincerely,

Kathleen L Kraninger

Kathleen L. Kraninger
Director

cc: The Honorable Chris Van Hollen, United States Senator
The Honorable Elizabeth Warren, United States Senator
The Honorable Jack Reed, United States Senator

Bureau of Consumer Financial Protection
1700 G Street NW
Washington, D.C. 20552

May 12, 2020

The Honorable Brian Schatz
United States Senate
722 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Schatz,

Thank you for your letter dated April 1, 2020, concerning the creation of a single federal resource for information on homeowner and renter relief provisions under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act). As you know, this is an evolving situation; as such we are continually monitoring and responding to new developments.

Today, with our partners at the Department of Housing and Urban and Development and the Federal Housing Finance Agency, we launched a dedicated portal on the Consumer Financial Protection Bureau's (Bureau's) website that provides unified guidance on housing related matters in response to COVID-19 pandemic. More specifically, the dedicated portal provides consumers with a single source for information about options to manage the housing impacts of the pandemic from these agencies and more.

The portal is designed to help consumers find assistance in three focus areas: mortgage relief, protection for renters, and how to avoid scams. It consolidates and streamlines content from each agency, so that consumers can quickly access the information most applicable to their personal circumstances. This includes resources to help homeowners determine the type of mortgage they hold and what relief options are available to them. It also includes information for renters to help determine whether CARES Act protections are available to them, and how to invoke them. The content on the portal will be translated into multiple other languages and is 508 compliant to ensure accessibility. The portal features links that enable users to quickly access other resources responsive to a wider range of concerns, including other resources on the COVID-19 pandemic. As the pandemic and our nation's response to it evolves, the portal will be updated periodically, with new content and functionality.

In this uncertain time, trusted, authoritative government sources are critical conduits for the distribution of information to the public. In closing, I would like to take this opportunity to ask that you share this resource with your constituents. Should you have any additional questions, please do not hesitate to contact me, or have your staff contact Kate Fink in the Bureau's Office of Legislative Affairs. Ms. Fink can be reached at (b) (6)

Sincerely,

Kathleen L Kraninger

Kathleen L. Kraninger
Director
Consumer Financial Protection Bureau

cc: The Honorable Sherrod Brown, United States Senator
The Honorable Bernard Sanders, United States Senator
The Honorable Jack Reed, United States Senator
The Honorable Elizabeth Warren, United States Senator
The Honorable Chris Van Hollen, United States Senator
The Honorable Michael F. Bennet, United States Senator
The Honorable Catherine Cortez Masto, United States Senator
The Honorable Robert Menendez, United States Senator
The Honorable Kyrsten Sinema, United States Senator
The Honorable Mazie K. Hirono, United States Senator
The Honorable Amy Klobuchar, United States Senator
The Honorable Richard J. Durbin, United States Senator
The Honorable Patty Murray, United States Senator
The Honorable Ron Wyden, United States Senator
The Honorable Margaret Wood Hassan, United States Senator
The Honorable Kirsten Gillibrand, United States Senator
The Honorable Gary C. Peters, United States Senator
The Honorable Dianne Feinstein, United States Senator
The Honorable Tina Smith, United States Senator

Bureau of Consumer Financial Protection
1700 G Street NW
Washington, D.C. 20552

May 18, 2020

The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing and Urban Affairs
United States Senate
534 Dirksen Senate Office Building
Washington, DC 20510

Dear Ranking Member Brown:

I write in response to your letter of May 4, 2020 based on a report in *The New York Times* regarding the Consumer Financial Protection Bureau's (Bureau's) rule on Payday, Vehicle Title, and Certain High-Cost Installment loans. Unfortunately, that reporting does not represent the robust process the Bureau engaged in to develop the 2019 Notice of Proposed Rulemaking (NPRM) much less the Bureau's process to consider public comments and finalize any rule.

In January 2018, the Bureau announced that it would undertake a rulemaking process to reconsider the November 2017 rule. Between January 2018 and February 2019, the Bureau thoroughly reviewed the evidence and legal analysis that underpinned the 2017 rule. On February 6, 2019, the Bureau released an NPRM seeking public review and comment on two proposed, preliminary determinations: first, the Bureau determined that the evidence underlying the identification of the unfair and abusive practice in the Mandatory Underwriting Provisions was not sufficient (more specifically, not sufficiently robust and reliable in light of the dramatic impacts the 2017 rule would have on consumers and the payday market); and second, the Bureau determined that the legal analysis underlying the 2017 Payday Rule for ascertaining whether a practice is unfair or abusive used a problematic approach. The Bureau explained the bases for these determinations and set a 90-day comment period. The Bureau received almost

200,000 public comments during this time, which have been posted to the public docket for this rulemaking. These comments include several hundred detailed comments from consumer groups, trade associations, non-depository lenders, banks, credit unions, research and advocacy organizations, members of Congress, industry service providers, fintech companies, Tribal leaders, faith leaders and coalitions of faith leaders, and State and local government officials and agencies. We also considered substantive comments received after the comment period closed, comments which of course were included in the public docket.

The Bureau has been engaged in a full consideration of the comments received, including comments addressing the initial economic analysis set forth in the NPRM. Upon my determination, the Bureau will issue a final rule on the basis of the record before the agency. And upon that basis, I will defend the agency's action.

I am immensely proud of the staff of the Bureau and continually impressed by their knowledge, passion, and dedication to the agency's mission. Within any organization, there will be differing opinions and viewpoints among staff. As such, I imagine there have been debates among staff in your offices and within *The New York Times* newsroom. With any major decision of the Bureau, as well as countless subsidiary decisions, there are often views and ideas competing for consideration. This results in thorough and informed debate and sometimes friction among Bureau staff of all levels, including among both career and political appointees. Staff at the Bureau know that I welcome this debate because rigorous policy evaluation and development generate better decisions and outcomes. They also respect that the decision regarding the agency's action, after considering the best advice and analysis the staff brings forward, ultimately rests with me as Director.

Should you have any questions about this response, please do not hesitate to contact me or have your staff contact Kate Fink in the Bureau's Office of Legislative Affairs. Ms. Fink can be reached at (b) (6)

Sincerely,

Kathleen L Kraninger

Kathleen L. Kraninger
Director

cc: The Honorable Elizabeth Warren, United States Senator
The Honorable Doug Jones, United States Senator
The Honorable Chris Van Hollen, United States Senator
The Honorable Catherine Cortez Masto, United States Senator
The Honorable Tina Smith, United States Senator
The Honorable Jack Reed, United States Senator
The Honorable Brian Schatz, United States Senator
The Honorable Jon Tester, United States Senator
The Honorable Robert Menendez, United States Senator
The Honorable Richard J. Durbin, United States Senator
The Honorable Mark R. Warner, United States Senator

Bureau of Consumer Financial Protection
1700 G Street NW
Washington, D.C. 20552

June 4, 2020

The Honorable Gregory Meeks
U.S. House of Representatives
2310 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Ayanna Pressley
U.S. House of Representatives
1108 Longworth House Office Building
Washington, D.C. 20515

Dear Congressman Meeks and Congresswoman Pressley:

Thank you for your letter dated May 1, 2020, regarding issues that some consumers have experienced with offsets to their economic impact payments. As the Consumer Financial Protection Bureau (Bureau) and our partner agencies take steps to support stability and public confidence in the nation's financial system in response to the COVID-19 health emergency, we appreciate this opportunity to update you on our efforts to prevent financial harm, help families who are struggling financially, and provide guidance to the financial industry to ensure their resources provide assistance to consumers in need.

The Bureau has taken a range of actions to provide guidance and flexibility to financial institutions on working with customers affected by COVID-19, including encouraging financial institutions to take prudent steps to work with consumers experiencing financial hardship. On April 13, 2020, the Bureau issued an interpretive rule to make it easier for pandemic-relief payments to be made on a prepaid debit card.[1] This rule facilitates pandemic relief payments to

[1] https://www.consumerfinance.gov/about-us/newsroom/cfpb-paves-way-consumers-receive-economic-impact-payments-quicker/.

consumers in a fast, secure, and efficient manner if direct deposit is unavailable. The Bureau also released a video and resources to inform consumers that they may receive their Economic Impact Payment on a prepaid debit card.[2] The Bureau has and will continue to actively engage with regulated entities, consumer advocates, State partners, and other stakeholders to ensure we are providing appropriate flexibilities to support consumers during this time.

In addition, the Bureau has taken numerous steps to protect and assist consumers during the COVID-19 national emergency, including informing consumers about their options with respect to mortgage forbearance; ensuring consumers will be able to continue to send remittance transfers without disruption; releasing a policy statement outlining the responsibilities of credit reporting companies and furnishers; and providing needed flexibility to enable financial companies to work with customers in need. To ensure homeowners and renters have the most up to date and accurate housing assistance information, the Bureau, the Federal Housing Finance Agency, and the Department of Housing and Urban Development recently launched a new mortgage and housing assistance website.[3] The Bureau has also released timely information on new programs aimed at helping struggling consumers during this time. These programs include stimulus payments;[4] student loan payment suspension;[5] mortgage forbearance;[6] and the paycheck protection program.[7] Additionally, the Bureau has a centralized webpage with information on how consumers can protect their finances during the pandemic.[8]

In this uncertain time, trusted, authoritative government sources are critical conduits for the distribution of information to the public. In closing, I would like to take this opportunity to ask

[2] https://www.consumerfinance.gov/coronavirus/managing-your-finances/economic-impact-payment-prepaid-debit-cards/; *and* https://www.consumerfinance.gov/about-us/blog/economic-impact-payment-prepaid-card/.

[3] https://www.cfpb.gov/housing.

[4] https://www.consumerfinance.gov/about-us/blog/guide-covid-19-economic-stimulus-checks/.

[5] https://www.consumerfinance.gov/about-us/blog/what-you-need-to-know-about-student-loans-and-coronavirus-pandemic/.

[6] https://www.consumerfinance.gov/about-us/blog/guide-coronavirus-mortgage-relief-options/.

[7] https://www.consumerfinance.gov/about-us/blog/help-small-businesses-during-covid-19-pandemic/.

[8] https://www.consumerfinance.gov/coronavirus/.

that you share the Bureau's resources with your constituents. Should you have any additional questions, please do not hesitate to contact me or have your staff contact Kate Fink in the Bureau's Office of Legislative Affairs. Ms. Fink can be reached at (b) (6)

Sincerely,

Kathleen L Kraninger

Kathleen L. Kraninger
Director