FY 20-21 Agency Priority Goal Action Plan

Strengthen Federal Cybersecurity

Goal Leader:

Matthew Hartman, Assistant Director (Acting), Cybersecurity Division, Cybersecurity and Infrastructure Security Agency

Overview

Goal Statement

- Protect federal networks by defending against threats and assisting agencies in managing risk. By September 30, 2021, 75% of critical and high configuration-based vulnerabilities identified through high value asset assessments will be mitigated within 30 days.

Challenges

- Variable agency capabilities and network architectures
- Network visibility limitations due to encryption and cloud computing
- Constantly evolving threat landscape and rapid pace of change in the cyber domain compared to the pace of federal government policy generation and implementation

Opportunities

- Empower DHS with additional authority to gain visibility into the federal enterprise and take action to safeguard systems
- Bring a unity of purpose to managing cybersecurity risks and protecting federal networks between DHS and agency network defense operators
- Ramp up use of coordinated tools and services to make federal networks more defensible and secure
- Synthesize risk posture data and assessments to reduce exposure to threats

Goal Strategies

Strategy 1: Increase Enterprise Risk Posture Awareness

Cybersecurity and Infrastructure Security Agency (CISA) will support departments and agencies to manage risk at an acceptable level, by tracking exposure to threats and heightening awareness of assets, users, and events on their networks to support risk-informed cybersecurity decisions and actions.

Understand the Environment
Identify and prioritize the most critical assets within the federal enterprise

Reduce Risk
Understand agencies' strategic risk postures through reporting and inputs from cybersecurity assessments

Strategy 2: Mitigate Known Vulnerabilities

CISA will deliver tools and technical support to fill critical gaps in agencies' cybersecurity capabilities and leverage policy directives and authorities to establish requirements and expectations for timely mitigation of vulnerabilities.

Provide Tools & Assistance
Offer assistance through tools and services, such as Continuous Diagnostics and Mitigation (CDM), cyber hygiene scanning, and high value asset assessments

Take Action
Strengthen cybersecurity posture and mitigate impacts

Strategy 3: Manage Malicious Incidents

CISA will defend the federal enterprise and target its efforts toward identifying and preventing the most significant threats through analysis, alerts, and intrusion detection and prevention technologies. Malicious activity will be mitigated and contained through collaboration with agency counterparts on cyber defense actions and direct response when needed.

Identify Threats
Detect and prevent malicious traffic

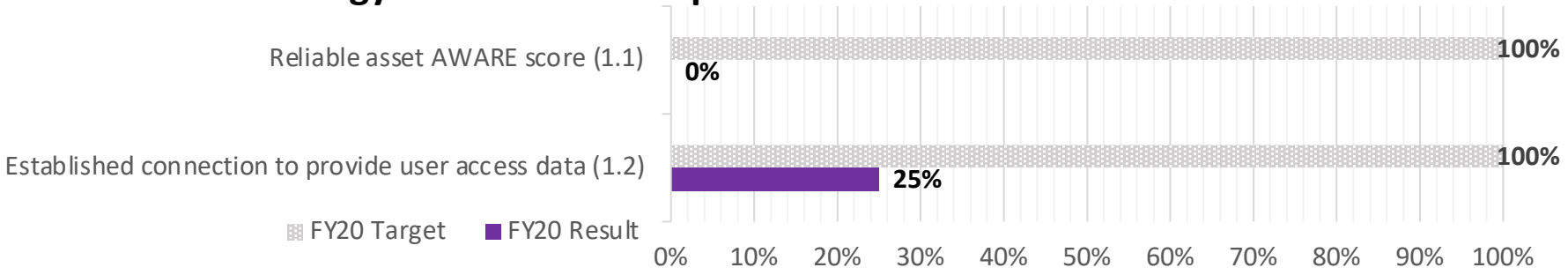
Respond to Incidents
Harness cross-cutting information from EINSTEIN, CDM, and other internal and external sources for agile analysis

Governance Approach for Remediation Escalation

Escalation Level	Remediation Timeline	Escalated By	Escalated To	CISA Action
6	Varies based on issue	Varies based on issue	Varies based on issue	If issue is not resolved by Escalation Level 5, CISA leadership and program staff work together to determine next escalation steps, including involvement by the DHS Deputy Under Secretary (DUS) and OMB. In-scope communication methods include phone call, prearranged meeting, or email notification with signed letter attached detailing escalation rationale.
5	10 business days after Escalation Level 4	CSD Assistant Director	Agency SAORM	CISA leadership facilitates escalation by CSD Assistant Director to agency Senior Agency Officials for Risk Management (SAORM) or equivalent. In-scope communication methods include phone call, prearranged meeting, or email notification with signed letter attached detailing escalation rationale.
4	10 business days after Escalation Level 3	CISA Leadership: Associate Director or Deputy Associate Director	Agency CIO	CISA management facilitates escalation by CISA leadership (Associate Director and/or Deputy Associate Director) to agency CIO. In-scope communication methods include phone call, prearranged meeting, or email notification with signed letter attached detailing escalation rationale.
3	5 business days after Escalation Level 2	CISA Management	Agency CISO	CISA program POC coordinates with CISA management and CISA Cyber Service Liaison (CSL) to notify agency CISO through email, phone call, or an arranged meeting (preferred method). CSL facilitates notification through established relationship with CISO and is included in notification and/or meeting.
2	5 business days after Escalation Level 1	CISA Program POC	Agency POC	CISA communicates past due date and outstanding action as second escalation by email notification or phone call to agency POC. Relevant CISA management included in communication, as applicable, and briefed as needed in preparation for potential action.
1	30-60 days after remediation is requested, or 1-2 days after defined deadline	CISA Program POC	Agency POC	CISA initiates escalation and communicates past due-date and outstanding action by email notification or phone call to agency POC.
0	1-30 days after remediation is requested, or other defined deadline	CISA Program POC	Agency POC	CISA articulates requested agency action and deadline and provides associated guidance and template, as relevant.

Key Indicators

Strategy 1: Increase Enterprise Risk Posture Awareness



#	Measure	Explanation
1.1	Percent of agencies for which a reliable Agency-Wide Adaptive Risk Enumeration (AWARE) score can be calculated for assets reporting to the Federal Dashboard	The first data certification cycle concluded in late July and certification scorecards were provided to relevant stakeholders. The CDM program presented its findings to agencies at the September CDM Customer Advisory Forum (CAF), along with a comprehensive plan to improve data quality. CDM portfolio teams are working with their respective agencies to establish action plans to implement corrective actions. Contributors to increased data quality included legacy Dashboard performance and tool configurations. CDM also hosted a virtual DEFENDer meeting with DEFEND integrators in late September; new data quality-related project tasks were discussed based upon the certification results. These tasks will involve more direct engagements with agency staff to acquire required datasets, expedite dashboard deployments, and coordinate tool access requirements. CDM's Architecture and Technology Integration Section Chief led a discussion on Data Quality Management observations at which CDM DEFEND integrators shared lessons learned from the first evaluation cycle and identified areas requiring agencies support. A second data certification cycle is planned for mid-FY21 and the program expects a handful of agencies to achieve data quality certification at that time. The process for increasing the remaining agencies will continue through FY21.
1.2	Percent of agencies who have established a data connection and begun providing user access data to the Federal Dashboard	A total of five CFO Act and 36 non-CFO Act agencies are reporting user access data to the Federal Dashboard as of the end of Q4 FY20. The Treasury, SSA, NASA, DOJ, and TVA joined the USDA, VA, DOI, GSA in reporting user access data to the integration layer and were waiting for the new Dashboard Ecosystem to be deployed to complete the user access data transfer with the Federal Dashboard. Once the new Dashboard Ecosystem is deployed then the results are expected to reach the 100% target.

Key Indicators

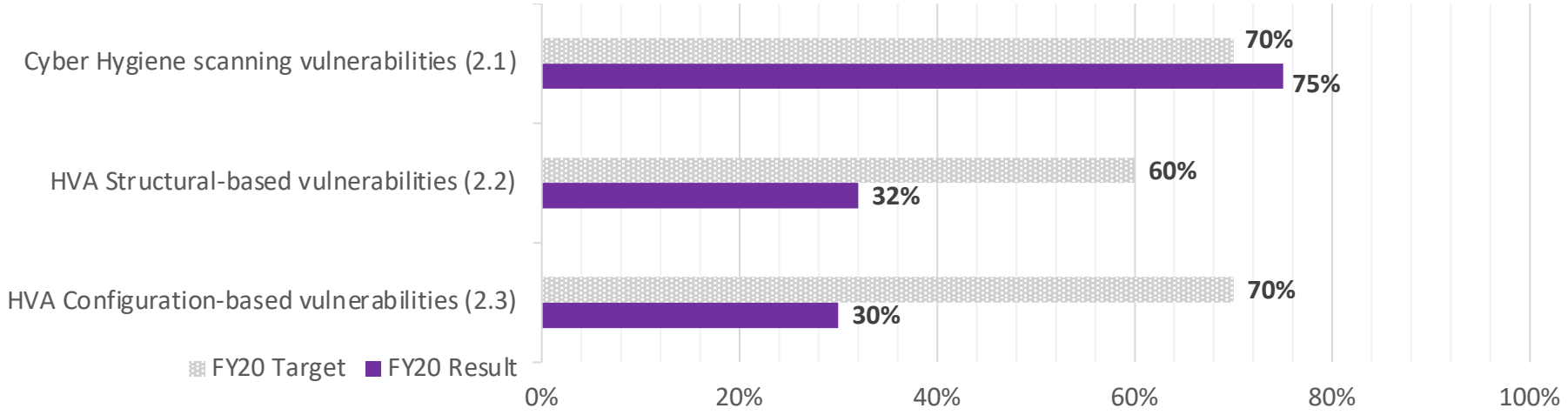
Strategy 1: Increase Enterprise Risk Posture Awareness

#	Measure	Explanation
1.3	Percent of agencies where IT hardware devices reported in the Federal Dashboard is within ten percent of agency self-reported numbers for Federal Information Security Management Act (FISMA) devices	**Reporting will begin in FY21**
1.4	Percent of agencies where the number of active users in the Federal Dashboard is within ten percent of agency self-reported numbers for FISMA users	**Reporting will begin in FY21**

Note: Measure descriptions are located in the Appendix (Table 1).

Key Indicators

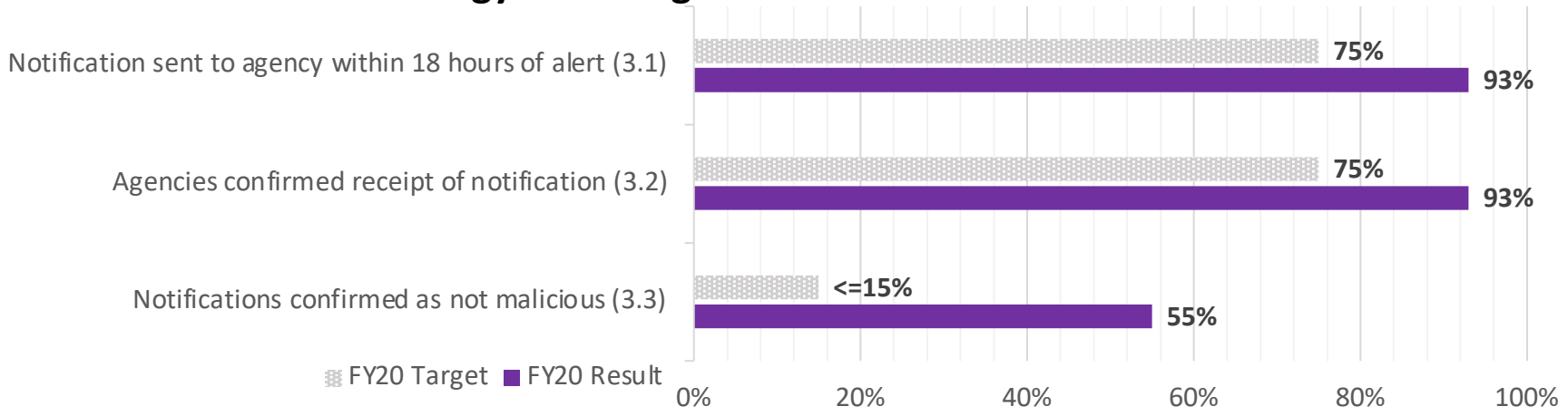
Strategy 2: Mitigate Known Vulnerabilities



#	Measure	Explanation
2.1	Percent of critical and high vulnerabilities identified through cyber hygiene scanning mitigated within the designated timeline	With Binding Operational Directive (BOD) 19-02 in effect since April 2019, agencies are demonstrating progress in addressing vulnerabilities within required timelines. Cumulative mitigation performance declined from Q3 to Q4, but in Q4, 343 critical and high vulnerabilities out of 488 vulnerabilities were remediated within the designated timeline.
2.2	Percent of mitigation activities for critical and high structural-based vulnerabilities identified through high value asset (HVA) assessments that are on schedule	As of Q4, there are 10 of 26 open structural-based findings identified during FY18-20 are on schedule. Structural-based findings are not on schedule due to Departments and Agencies not submitting remediation plans or meeting approved mitigation timelines. The following agencies have open structural-based vulnerabilities: TREAS, DOS, EPA, SEC, USDA, SSA, OPM, DOI, DOT, and HUD.
2.3	**Key Measure: Percent of critical and high configuration-based vulnerabilities identified through high value asset assessments mitigated within 30 days**	During FY20, 6 out of 20 configuration-based vulnerabilities identified on high value assets were mitigated within the 30-day timeline. There were no new Risk and Vulnerability Assessments (RVAs) in Q4, therefore no configuration-based findings were identified.

Key Indicators

Strategy 3: Manage Malicious Incidents



#	Measure	Explanation
3.1	Percent of potential malicious cyber activity notifications where impacted agencies were alerted within the specified timeframe	During FY20, 93% of notifications were sent out within the 18-hour window, surpassing the target. For the last quarter of FY20, there were three notifications, with two sent out within the 18-hour window.
3.2	Percent of potential malicious cyber activity notifications where the notified agency confirms receipt	During FY20, 93% of agencies confirmed receipt of notifications, again surpassing the target. For the last quarter of FY20, each of the three notifications were confirmed as received by the agencies.
3.3	Percent of potential malicious cyber activity notifications confirmed by agencies as not malicious	During FY20, 55% of notifications sent to agencies were determined by agencies as not malicious, a result much higher than the target. False positives are often caused by security appliances, sandboxes, and guest networks. There are approximately 8 notifications sent per quarter, so the volume is small. The result furthers the programs ongoing goal to gain visibility into the networks of Departments and Agencies.

Summary of Progress

Strategy	Progress Update
1. Increase Enterprise Risk Posture Awareness	• CDM data quality continues to present a challenge. The CDM program completed its first Data Quality Submission/Certification Cycle (SC-1) at the end of July and provided results to agencies and key stakeholders. Although no agencies met the certification criteria, a handful were close. Several key findings were identified that contribute directly to data quality, including: ○ Legacy CDM Dashboard Performance ○ CDM Tool Configuration ○ Missing FISMA container data ○ Agency deployment scheduling/status ○ Uncoordinated (lengthy) agency outages The CDM program presented the SC-1 results and findings to agencies in mid-September at the Customer Advisory Forum (CAF), along with a comprehensive plan to improve data quality. CDM portfolio teams are working with their respective agencies to establish action plans to implement corrective actions. The program is also working with CDM integrators to quickly identify and mitigate obstacles and impediments at agencies in order to get resolution in a timely manner. • For Identity & Access Management, CDM integrators have shifted their time to focus on the rollout of the new Dashboard Ecosystem and retirement of the legacy Archer dashboard. Efforts to carry user access data up to the Dashboard layers will ramp back up once the new Dashboard Ecosystem has been deployed; CDM expects to complete this transition and enable summary user access data reporting at the Federal Dashboard by the end of FY21.

Summary of Progress

Strategy	Progress Update
2. Mitigate Known Vulnerabilities	The HVA Risk and Solution Analysis is complete, and the team has mapped the risks to CISA services, solutions, capabilities, and offerings. CISA has identified the agency specific risks for most of the CFO-act agencies. CISA has prioritized the risks and determined the best path forward to assist the Federal Civilian Executive Branch agencies in reducing the risks holistically. Many of these risks are long-term systemic issues that will take years to develop the approach for agencies to reduce the risks.
3. Manage Malicious Incidents	CISA continues to work on the Collaborative Host Analysis and Mitigation Project (CHAMP) pilot effort. The intention of CHAMP is to gain additional visibility into the Departments' and Agencies' (D/A) hosts regarding potential alerts. The initiative aims to work with agencies to confirm whether what is observed at the perimeter aligns with what is observed at the host level inside the network. This additional visibility within the D/As provides more information about potential issues and will help CISA gain additional fidelity before reaching out to a D/A Security Operating Center (SOC). The effort also may enhance CISA's ability to inform the D/A about which machine(s) are compromised.

Key Milestones

Strategy 1: Increase Enterprise Risk Posture Awareness

#	Key Milestone	Due Date	Status	Comments
M.1.1	Complete survey of agency asset reporting at the CDM Federal Dashboard, evaluate against authoritative, reported data, and notify agencies of results	FY20, Q1	Complete	The CDM PMO reviewed the agency asset reporting at the CDM Federal Dashboard level and evaluated it against the agency CDM asset discovery data and the reported FISMA data for FY19. The CDM PMO Architecture and Technology Integration Section developed a Data Quality Management Plan (DQMP) that addresses the approach for validating agency asset counts, as well as ensuring the data quality (e.g., vulnerability and configuration information) associated with those assets. The CDM PMO met with the CDM system integrators to discuss the direction for data quality and met with the agencies in January during the CDM Customer Advisory Forum to discuss the current asset counts and the plan for ensuring the quality of those asset counts.
M.1.2	Develop and implement data quality improvement protocols and execution plan in collaboration with agencies	FY20, Q2	Complete	The CDM PMO developed its DQMP with agencies and system integrators, which began with a top-to-bottom architecture review of CDM solutions to conduct system analysis focused on data quality. The CDM PMO representatives and system integrators ran a series of "dry-run" surveys with agency data sets to prove out assessment processes and criteria. Results were analyzed to inform the data certification process and were completed by the end of April. Full-scale quality reviews began in May and continue through the remainder of the fiscal year.
M.1.3	Validate agency summary asset reporting results on the CDM Federal Dashboard against agency authoritative asset reports	FY20, Q3	Complete	The CDM program finalized the results of the initial data quality survey conducted in Q2 and published the certification process to all CDM DEFEND integrators and agency partners at the end of May. The CDM program stood up a centralized, automated DHS-hosted ticketing system to track quality issues as they are identified. Data quality assessments began in late June with discrepancies (i.e. tickets) being recorded and issued directly to DEFEND integrators for remediation. The first data quality evaluation window will conclude in late July with results provided to relevant stakeholders.

Key Milestones

Strategy 1: Increase Enterprise Risk Posture Awareness

#	Key Milestone	Due Date	Status	Comments
M.1.4	Complete delivery and integration of agency user access management tools with agency dashboards, and verify agency summary user access management data exchanges with the Federal Dashboard	FY20, Q4	Missed	The CDM program currently has five CFO Act agencies and 36 non-CFO Act agencies reporting user access data to the Federal Dashboard, plus an additional nine agencies reporting data to the CDM data integration layer and prepared to begin exchanging user access data once the new CDM Dashboard Ecosystem has been deployed at those agencies. The CDM program projects that the remaining agencies' user access tools will be completed in FY21, as will the transition to the new Dashboard Ecosystem.

Key Milestones

Strategy 2: Mitigate Known Vulnerabilities

#	Key Milestone	Due Date	Status	Comments
M.2.1	Implementation of improved process to integrate CDM, the Quality Service Management Office (QSMO), HVA, and Vulnerability Management support during engagements and out-briefs to provide enhanced technical support to agencies for remediation of vulnerabilities	FY20, Q1	Complete	Once assessment reports are drafted, relevant CISA program offices are notified so they can review the reports to identify any potential actions by their teams to address vulnerabilities utilizing current CISA services, QSMO offerings, or cyber engineering support. Critical and Major/High risks take priority over moderate or information risks. Relevant program offices participate in the internal and external risk briefs to ensure early engagement with agencies in their remediation processes. CISA's HVA and CDM teams are working together to proactively define technical capabilities aligned to the most common findings, so remediation support can be executed more quickly. CISA also continues to engage agencies in the CDM Data protection pilots to quickly address risks. These engagements are still in the early phase, and CISA continues to reach out to agencies to work with them in applying already outlined capabilities against known historical findings.
M.2.2	Accelerate and enhance escalation process for missed remediation plan dates progressively up the agency's leadership chain	FY20, Q2	Complete	The CISA Cyber Directives team has revised the escalation process and received approval to utilize this moving forward. The Directives team closely tracks Agency compliance and utilizes internal tools to monitor necessary and ongoing escalations. Escalations have proven useful to receive materials from the agency and closing out open findings faster.
M.2.3	Completion of a gap analysis of common risks compared with CISA offerings and solutions	FY20, Q3	Missed	CISA has developed a matrix of HVA risks as compared to current CISA offerings. This information is used for several reasons to provide appropriate services and solutions to agencies to reduce identified risks. Likewise, CISA will identify any gaps in the offerings to determine what services, solutions, guidance, directives, etc. that CISA should consider adding to our services.

Note: Milestone Status Definitions are located in the Appendix (Table 2).

Key Milestones

Strategy 2: Mitigate Known Vulnerabilities

#	Key Milestone	Due Date	Status	Comments
M.2.4	Create and implement a process to leverage Plan of Action and Milestones (POA&M) information to build an agency-focused profile of remediation efforts, systemic challenges, reoccurring issues, cycle times of vulnerabilities, outliers, and other aspects of vulnerability management to allow CISA to make informed decisions on assistance to the agencies	FY20, Q4	Complete	CISA has created Agency Support Plans for most of the CFO Act agencies based on the data CISA has access to from assessments, data collections, directives, and other technical sources. These support plans identify remediation efforts, challenges, issues, for these agencies. CISA consolidates this information into Federal Civilian Executive Branch-wide systemic risks and issues to drive CISA services, solutions, efforts, products, workshops, etc. to assist in the reduction of the federal risk.

Note: Milestone Status Definitions are located in the Appendix (Table 2).

Key Milestones

Strategy 3: Manage Malicious Incidents

#	Key Milestone	Due Date	Status	Comments
M.3.1	Modifications to Standard Operating Procedures (SOPs) for notification and tracking of reported potential incidents complete	FY20, Q1	Complete	The SOP was created and implemented, but there were some refinements identified that CISA addressed in Q2 to improve the process further.
M.3.2	Verification and update of agency Security Operations Center (SOC) contact information launched	FY20, Q2	Complete	CISA worked in Q1 and Q2 to verify and update SOC contact information. This process to verify and update SOC contact information is believed to have contributed to the increase in agency responses from Q1 to Q2.
M.3.3	Verification and update of agency SOC contact information completed	FY20, Q3	Complete	CISA worked from Q1 to Q3 to verify and update SOC contact information. This process to verify and update SOC contact information is complete and believed to have contributed to the increase in agency responses from Q1 to Q3.
M.3.4	Feedback from agencies on how they analyze and respond to notifications of potential malicious incidents received	FY20, Q4	Complete	CISA engaged with many departments and agencies (D/A) and each D/A Security Operations Center (SOC) addressed CISA reports (INARs) in a different or slightly different way. One of the reoccurring issues from both CISA/CSD, as well as the other D/As, was false positives were based on security appliances or other known network elements. We have been working to compile a list of known devices (security appliances) or networks (guest networks) to better inform our analysis. This process will be dynamic, because no D/As network is truly static. In a future state, it would be best if this process could be automated, but at this time manual scans and data calls would be the method for better understanding the D/As.

Note: Milestone Status Definitions are located in the Appendix (Table 2).

Contributing Programs & Stakeholders

Contributing Programs

- Cybersecurity Division (CSD), DHS/CISA
- DHS Office of the Chief Information Security Officer (OCISO)
- Federal Civilian Executive Branch Agencies
- Agency Security/Network Operations Centers (SOC/NOC)

Stakeholders

- Federal Civilian Executive Branch Agencies
- Federal Chief Information Officers (CIOs)
- Federal Chief Information Security Officers (CISOs)
- Office of Management and Budget (OMB)
- Congress
- Government Accountability Office (GAO)
- Agency Inspectors General (IGs)
- The American Public

Appendix

APG Measure Descriptions and Milestone Status Definitions

Additional information on the performance measure data accuracy and reliability are available at:
DHS FY19-21 Annual Performance Report Appendix A

Appendix

Table 1: Measure Descriptions

Measure Name	Measure Description
1.1 Percent of agencies for which a reliable Agency-Wide Adaptive Risk Enumeration score can be calculated for assets reporting to the Federal Dashboard	This measure reports the percent of participating federal agencies that have established a reliable active Continuous Diagnostics and Mitigation (CDM) connection with the Federal Dashboard allowing the calculation of an Agency-Wide Adaptive Risk Enumeration (AWARE) score. Reliable AWARE scores use numerical scales to quantify the severity of identified vulnerabilities of IT systems (assets), how long they have been present, and the impact to these systems. This measure is an indicator of agencies' cybersecurity posture, and their ability to provide information to the Federal Dashboard to identify system vulnerabilities. AWARE scores serve as a mechanism to prioritize and remediate system vulnerabilities.
1.2 Percent of agencies who have established a data connection and begun providing user access data to the Federal Dashboard	This measure reports the percent of participating federal civilian executive branch agencies where they have established an active Continuous Diagnostics and Mitigation (CDM) connection with the Federal Dashboard and begun providing user access and privilege information. The value being counted is whether any one of the agencies' organizations is providing user access and privilege information to the Federal Dashboard. The user access and privileged information being gauged relates to Identity and Access Management (formerly Phase Two) of the CDM tools reflecting "who is on the network" and demonstrates the successful deployment, integration, display and exchange of data. The measure gauges implementation progress for restricting network privileges and access to only those individuals who need it to perform their duties on federal networks.
1.3 Percent of agencies where IT hardware devices reported in the Federal Dashboard is within ten percent of agency self-reported numbers for Federal Information Security Management Act devices	This measure reports the percent of participating federal agencies with an active Continuous Diagnostics and Mitigation (CDM) connection with the Federal Dashboard whose automated collection of the number of hardware devices is within ten percent of the agency's self-report Federal Information Security Management Act (FISMA) device numbers. Currently due to complexities with automated detection along with the status of CDM implementation, device data can vary significantly for federal agencies. This measure provides an indicator of the extent of this deviation and is intended to drive attention to addressing and resolving these differences and improve data integrity.
1.4 Percent of agencies where the number of active users in the Federal Dashboard is within ten percent of agency self-reported numbers for Federal Information Security Management Act users	This measure reports the percent of participating federal agencies with an active Continuous Diagnostics and Mitigation (CDM) connection with the Federal Dashboard whose automated collection of the number of active users is within ten percent of the agency's self-report Federal Information Security Management Act (FISMA) users. Currently due to complexities with automated detection along with the status of CDM implementation, user data can vary significantly for federal agencies. This measure provides an indicator of the extent of this deviation and is intended to drive attention to addressing and resolving these differences and improve data integrity.

Appendix

Measure Name	Measure Description
2.1 Percent of critical and high vulnerabilities identified through cyber hygiene scanning mitigated within the designated timeline	This measure calculates the percent of critical and high vulnerabilities, identified through cyber hygiene scanning, that have been mitigated within the specified timeline. Cyber scanning occurs in federal agencies and departments but does not include the Department of Defense or the Intelligence Community. For critical vulnerabilities, mitigation is required within 15 days from point of initial detection, and for high vulnerabilities mitigation is required within 30 days. Cyber hygiene scanning prioritizes vulnerabilities based on their severity as a means for agencies to make risk-based decisions regarding their network security. Identifying and mitigating vulnerabilities on a network in a timely manner is a critical component of an effective cybersecurity program, as it is critical to maintaining operational availability and integrity of IT systems.
2.2 Percent of mitigation activities for critical and high structural-based vulnerabilities identified through high value asset assessments that are on schedule	This measure reports the percent of mitigation activities federal agencies and departments have established to resolve critical and high structural vulnerabilities identified in High Value Assets (HVA) asset assessments that are on schedule. HVA assessments are performed across the Federal Government to identify vulnerabilities associated with the most sensitive IT systems and data. Structural-based vulnerabilities are those that have adverse impact across multiple business units and require long-term and detailed planning, procurement, integration, and testing to be mitigated (such as network segmentation, data loss prevention, and data encryption). Ensuring mitigation activities stay on schedule ensure agencies and departments are on track and dedicating resources to mitigate structural-based vulnerabilities so as to protect the Federal Government's most sensitive IT systems and data.
2.3 Percent of critical and high configuration-based vulnerabilities identified through high value asset assessments mitigated within 30 days	This measure reports the percent of critical and high configuration-based vulnerabilities identified in High Value Assets (HVA) assessments that have been mitigated within 30 days. HVA assessments are performed across the Federal Government to identify vulnerabilities associated with the most sensitive IT systems and data. Configuration-based vulnerabilities are those that can be more quickly be mitigated by agencies and departments through such actions as changing security settings, software or configuration changes, patching software vulnerabilities, and adjusting user account privileges. Agencies and departments report monthly to the program on the status of mitigating these configuration-based vulnerabilities. The results indicate if agencies and departments are resolving less complex HVA vulnerabilities within the government-wide goal of 30 days.
3.1 Percent of potential malicious cyber activity notifications where impacted agencies were alerted within the specified timeframe	The measure tracks the percent of potential malicious cyber activity notifications identified as credible where the affected agency is alerted within the specified timeframe. Potential malicious cyber activity on federal networks is detected by automated tools through the National Cyber Protection System (NCPS) alert-based detection function. The system sends automated notifications to analysts within NCPS, who then manually review the notification(s), confirm if a potential credible threat exists, and if so, the affected agency is sent a notification by email for their further exploration. The specified timeframe to notify affected agencies of potential malicious cyber activity is 18 hours for FY20 and 12 hours for FY21.

Appendix

Measure Name	Measure Description
3.2 Percent of potential malicious cyber activity notifications where the notified agency confirms receipt	This measure tracks all the potential malicious cyber activity notifications that were sent to agencies where the notified agency acknowledges receipt. Potential malicious cyber activity on federal networks is detected by automated tools through the National Cyber Protection System (NCPS) alert-based detection function. The system sends automated notifications to Computer Network Defense (CND) analysts within NCPS, who then manually review the notification(s), confirm if a potential credible threat exists, and if so, the affected agency is sent an email for their further exploration. This measure provides confirmation to the program that the notification has been received.
3.3 Percent of potential malicious cyber activity notifications confirmed by agencies as not malicious	This measure tracks all the potential malicious cyber activity notifications that were sent to agencies where the notified agency confirmed the activity as not malicious. Potential malicious cyber activity on federal networks is detected by automated tools through the National Cyber Protection System (NCPS) alert-based detection function. The system sends automated notifications to analysts within NCPS, who then manually review the notification(s), confirm if a potential credible threat exists, and if so, the affected agency is sent an email notification for their further exploration. Upon receipt of the notification, agencies investigate the potential malicious activity and communicate back to the program if the notification pertained to non-malicious activity. This measure provides an indicator of the precision of the diagnosis process.

Table 2: Milestone Status Definitions

Milestone Status	Definition
Unscheduled	Specific activities to meet the milestones have not been determined
Scheduled	Specific activities to meet the milestone have been determined
On Track	Specific activities to meet the milestone have started
Complete	Milestone has been accomplished by due date
Missed	Milestone was not accomplished by due date