TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Systems Processing Economic Impact Payments Performed Well and the Get My Payment Application Security Vulnerabilities Are Being Remediated

December 28, 2020

Report Number: 2021-26-006

TIGTACommunications@tigta.treas.gov | www.treasury.gov/tigta | 202-622-6500

HIGHLIGHTS: Systems Processing Economic Impact Payments Performed Well and the Get My Payment Application Security Vulnerabilities Are Being Remediated

Final Audit Report issued on December 28, 2020
Report Number 2021-26-006

Why TIGTA Did This Audit

This audit was initiated to review the effectiveness of IRS systems security and operations related to processing the Coronavirus Aid, Relief, and Economic Security Act Economic Impact Payments.

Impact on Taxpayers

On March 27, 2020, the Coronavirus Aid, Relief, and Economic Security Act, which is the largest economic rescue package in U.S. history, was signed into law. The Act directed the IRS to deliver Economic Impact Payments to eligible individuals, in addition to containing numerous tax-related provisions for both individuals and businesses. The Act appropriated $750.7 million in additional funding to the IRS to administer and oversee these provisions.

On April 10, 2020, the IRS issued more than 81.4 million payments totaling more than $147.6 billion. As of September 25, 2020, the IRS issued more than 165 million Economic Impact Payments totaling more than $276 billion.

What TIGTA Found

Overall, the 16 IRS tax systems involved in delivering Economic Impact Payments to individuals performed well. However, a coding issue in the software developed to process the payments affected the Individual Master File's performance. The IRS fully restored the system within approximately 24 hours and the affected payments were processed the following business day.

TIGTA determined that 463 (99 percent) of 470 required baseline security controls and control enhancements were implemented for the Get My Payment application. The security controls not implemented related to vulnerability scanning, flaw remediation, information input validation, cryptographic protection, and information system component inventory. In response to these findings, the Applications Development function opened a Plan of Action and Milestones to address each deficiency. However, the IRS failed to timely remediate 17 critical (four unique) and 169 high (five unique) security vulnerabilities that were identified in the Get My Payment application database.

Lastly, the IRS assessed the Get My Payment application's appropriate identity and authenticator assurance levels at level two, higher than the currently implemented level one. Although the IRS implemented identity and authenticator assurance levels below the assessed level, TIGTA found that the Digital Identity Acceptance Statement met the National Institute of Standards and Technology and agency requirements by including a detailed implementation and rationale, compensating controls and risk mitigation factors, a description of risk acceptance, and a plan of action.

What TIGTA Recommended

The Chief Information Officer should ensure that critical and high security vulnerabilities are timely remediated based on agency-defined timelines, and Plans of Action and Milestones associated with the Get My Payment application are completed timely based on agency defined timelines and processes.

The IRS agreed with both recommendations. The IRS plans to remediate the critical and high vulnerabilities as well as the Plans of Action and Milestones identified in the audit.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

December 28, 2020

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: M. Weir for
Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Systems Processing Economic Impact Payments Performed Well and the Get My Payment Application Security Vulnerabilities Are Being Remediated (Audit # 202020626)

This report presents the results of our review to review the effectiveness of Internal Revenue Service (IRS) systems security and operations related to the Coronavirus Aid, Relief, and Economic Security Act Economic Impact Payment processing. This review is part of our Fiscal Year 2021 Annual Audit Plan and addresses the major management and performance challenge of *Responding to the COVID-19 Pandemic*.

Management's complete response to the draft report is included as Appendix II.

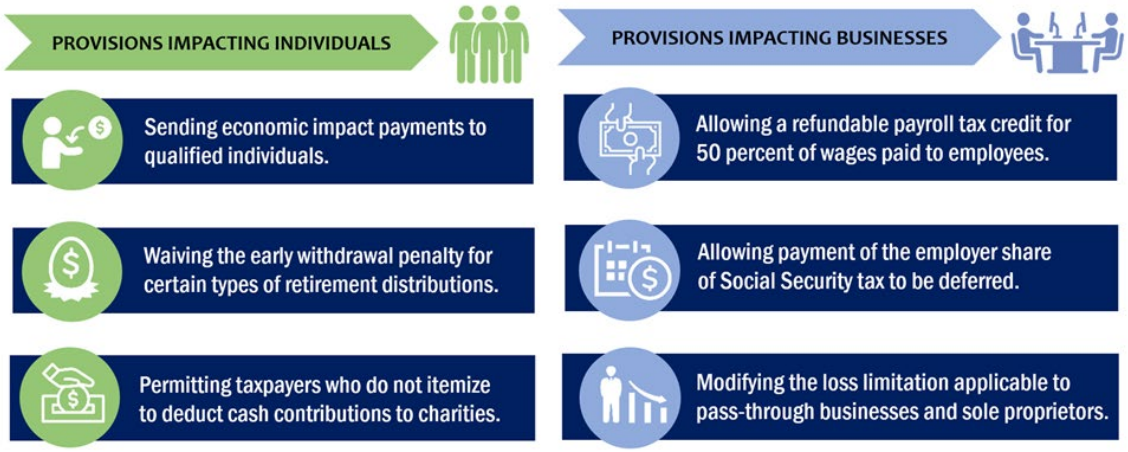
Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background

On March 27, 2020, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act)[1] was signed into law. The CARES Act is the largest economic rescue package in U.S. history and will have a significant impact on the Internal Revenue Service (IRS) and Federal tax administration. The CARES Act contains numerous tax-related provisions affecting individuals and businesses and appropriated $750.7 million[2] in additional funding to the IRS to administer and oversee these provisions. Figure 1 summarizes the CARES Act Provisions.

Figure 1: Highlights of the CARES Act Provisions



Source: Treasury Inspector General for Tax Administration analysis of the CARES Act.

With more than 56,000 IRS employees teleworking due to the closure of more than 90 percent of all IRS facilities, the IRS faced significant challenges because of the Coronavirus-19 pandemic.

The IRS expedited its analysis and reprogramming of systems and educated taxpayers on Economic Impact Payments. The IRS began issuing Economic Impact Payments on April 10, 2020, just 14 days after the passage of the CARES Act; at the same time, the IRS was closing its facilities in response to the Coronavirus-19 pandemic. In order to complete this task, the IRS established a dedicated web page on IRS.gov to provide updated information related to the issuance of Economic Impact Payments, including a continually evolving list of frequently asked questions.

The IRS also coordinated with other Federal agencies to obtain program data that could automatically send Economic Impact Payments to individuals who receive benefits from these agencies and do not regularly interact with the IRS. For example, the IRS worked with the Bureau of the Fiscal Service,[3] the Social Security Administration, and the Department of Veterans Affairs to identify beneficiary recipients along with their direct deposit account numbers.

[1] Pub. L. No. 116-136, 134 Stat. 281.
[2] The IRS was appropriated $293.5 million for Taxpayer Services, $250 million to prevent, prepare for, and respond to Coranavirus-19, including implementation of the CARES Act, $170 million for Operations Support, and $37.2 million for Enforcement.
[3] An agency of the U.S. Department of the Treasury that issues payments on behalf of the IRS.

As a result, the IRS issued more than 81.4 million payments totaling more than $147.6 billion on April 10, 2020. As of September 25, 2020, the IRS issued more than 165 million Economic Impact Payments totaling more than $276 billion.

Results of Review

Tax Systems Involved in Delivering Economic Impact Payments to Individuals Generally Performed Well

The CARES Act provisions which provide economic relief to individuals include the issuance of recovery rebates of $1,200 per eligible individual ($2,400 in the case of eligible individuals filing a joint return) and $500 for each qualifying child. The Joint Committee on Taxation estimated the cost of the rebate provision to be approximately $292.4 billion over Fiscal Years 2020 and 2021.[4]

To support these efforts, despite office closures and employees working remotely, the IRS completed extensive computer programming and testing that was necessary to begin issuing the Economic Impact Payments. This included developing computer programming requirements to identify eligible individuals, compute their Economic Impact Payment amounts, as well as modify the Individual Master File[5] to capture information related to the issuance of the Economic Impact Payment in each individual's tax account. In total, 16 IRS tax systems were involved in the processing and delivery of the Economic Impact Payments to individual taxpayers.

Of these 16 IRS tax systems, only the Individual Master File experienced a performance problem due to a coding issue in the software developed to process the payments. The IRS fully restored the system within approximately 24 hours and the Economic Impact Payments scheduled to be delivered during the outage were processed the following business day.

By quickly restoring the Individual Master File functionality, the IRS was able to continue to timely issue the Economic Impact Payments to individual taxpayers in accordance with the CARES Act.

Most Required Baseline Security Controls Were Implemented for the Get My Payment Application

The National Institute of Standards and Technology (NIST) provides guidelines[6] to select and specify security controls for organizations and information systems, which support the executive agencies of the Federal Government, to ensure that they meet the minimum requirements of

[4] JCX-11-20 (March 26, 2020).

[5] See Appendix III for a glossary of terms.

[6] NIST Special Publication 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013). Revision 5 of this publication was released in September 2020. We assessed the Get My Payment application against the controls required during our audit fieldwork. Because we concluded our analysis in August 2020, we used the criteria established in Revision 4.

the Federal Information Processing Standards.[7] These guidelines apply to all components of an information system that process, store, or transmit Federal information.

The Internal Revenue Manual (IRM)[8] establishes the security framework for the development of security control specific implementations defined in subordinate IRMs, IRS publications, and other subordinate procedural guidance. The IRM also requires that all information systems be assigned a Federal Information Processing Standards Security Impact-level Designator.[9] Federal Information Processing Standards Security Impact-level Designators are:

- (L) – Applies to systems categorized as Impact-level LOW.
- (M) – Applies to systems categorized as Impact-level MODERATE.
- (H) – Applies to systems categorized as Impact-level HIGH.

On April 15, 2020, the IRS launched the Get My Payment (GMP) application, a web-based tool that provides taxpayers with the ability to check the status of their Economic Impact Payments and submit missing bank information for their accounts. The GMP application is part of the Integrated Customer Communications Environment (ICCE), which is comprised of numerous web and telephone applications. The functionality of these automated self-service applications supports the IRS mission by providing taxpayers with a variety of services, such as the ability to check tax refund status and establish payment agreements. Each of these taxpayer-facing, interactive applications are currently operational. The ICCE, including the GMP application, is designated as an Impact-level MODERATE system.

Agency security policies require that security controls be documented and assessed for a system's initial authorization, updated and assessed annually for a system's continued authorization, and updated and assessed on an ad-hoc basis resulting from significant changes performed on the system.[10] According to Cybersecurity function officials, the addition of the GMP application to the ICCE was a significant change to the system and triggered an Event-Driven Security Controls Assessment.

We determined that 470 NIST and agency-specific security controls and control enhancements were applicable to the GMP application. We found that 463 (99 percent) of 470 applicable security controls and control enhancements were fully implemented. Figure 2 provides a summary of the GMP security controls implementation.

[7] Department of Commerce, Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems Publication* (Mar. 2006).
[8] IRM 10.8.1, *Information Technology Security, Policy and Guidance* (May 9, 2019).
[9] Department of Commerce, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004).
[10] IRS, *Federal Information Security Modernization Act Security Controls Assessment Standard Operating Procedure* (Feb. 7, 2020).

Figure 2: Summary of GMP Application Security Controls Implementation (Number of controls implemented)

Control Family	Applicable Security Controls	Security Controls Implemented	Security Controls Not Implemented
Access Control	32	32	0
Audit and Accountability	27	27	0
Awareness and Training	11	11	0
Configuration Management	42	39	3
Contingency Planning	39	39	0
Identification and Authentication	18	18	0
Incident Response	23	23	0
Maintenance	22	22	0
Media Protection	16	16	0
Personnel Security	28	28	0
Physical and Environmental Protection	37	37	0
Planning	16	16	0
Risk Assessment	18	17	1
Security Assessment and Authorization	26	26	0
System and Communications Protection	34	33	1
System and Information Integrity	41	39	2
System and Services Acquisition	40	40	0
Totals	**470**	**463**	**7**

Source: Treasury Inspector General for Tax Administration analysis of the GMP application's Baseline Security Controls.

The four control family categories identified in Figure 2 as having controls not implemented contained specific risk areas that need to be addressed. The IRS documented an active Plan of Action and Milestones (POA&M) for each risk area to reduce these risks, ensure system integrity, and maximize system availability for taxpayers.

Critical and high security vulnerabilities were not timely remediated

To satisfy the NIST security control requirement for Vulnerability Scanning (Risk Assessment control family), the IRM requires system owners to deploy vulnerability scanning tools that look for software flaws and improper configurations and measure vulnerability impacts. The IRM also requires information systems to be scanned at least monthly for vulnerabilities. We found that the IRS has successfully deployed the necessary tools and implemented procedures to detect software vulnerabilities for the GMP application. The IRM also states that legitimate vulnerabilities shall be remediated in accordance with agency-approved response times based on the severity level of the vulnerability. Vulnerabilities with the highest risk shall be prioritized

and remediated first. Common Vulnerability Scoring System scores provided by the scanning tools shall be used to prioritize vulnerabilities. Figure 3 shows the score ranges and their associated remediation time frames.

Figure 3: Common Vulnerability Scoring System Ranges by Severity Risk Level and Remediation Time Frames

Score Range	Vulnerability Severity Risk Level	Remediation Time Frame
0.0	None	None
0.1-3.9	Low	180 days
4.0-6.9	Medium	120 days
7.0-8.9	High	High Value Assets = 60 days All other systems = 90 days
9.0-10.0	Critical	30 days

Source: IRM 10.8.1.

On June 25, 2020, the IRS provided the May 2020 database vulnerability scan report for the ICCE, which houses the GMP application. Based on our evaluation of the report, we determined the following:

- There were a total of 186 critical and high vulnerabilities; 17 critical (four unique) vulnerabilities and 169 high (five unique) vulnerabilities.
  - All 17 critical vulnerabilities exceeded the IRS policy of 30 days for remediation.
  - All 169 high vulnerabilities exceeded the IRS policy of 90 days for remediation.
- That nine (53 percent) of the 17 critical vulnerabilities have existed for more than 180 days, of which four had a first-failed date of October 2, 2018.
- That 121 (72 percent) of the 169 high vulnerabilities have existed for nearly 590 days, of which 105 had a first-failed date of October 2, 2018.

In addition, in the June 2020 GMP application's Security Assessment Report,[11] the Cybersecurity function's Security Risk Management office issued a finding to the ICCE Authorizing Official stating that the database vulnerability scan reports identified 17 critical and 169 high security vulnerabilities. The IRS assessed the likelihood of a threat exploiting these vulnerabilities as high, the impact of a threat exploiting these vulnerabilities as moderate, and assessed the overall risk level associated with these vulnerabilities as moderate.

During the course of the audit, the IRS had completed multiple actions in an effort to resolve these findings, including the installation of required database patches, coordination with database administrators from the Enterprise Operations function to develop a hardening script, and deployment of the script to the production database. However, we determined that due to multiple competing priorities and time constraints, the IRS did not timely remediate these vulnerabilities within agency-defined time frames.

Failing to timely remediate critical and high security vulnerabilities could compromise the security posture of the GMP application's database and can lead to unauthorized access,

[11] IRS, *Get My Payment Tier 2 Security Assessment Report* (June 10, 2020).

increased vulnerability to attacks, and unauthorized data sharing, all of which compromise the integrity, confidentiality, and availability of the system.

Management Action: On June 18, 2020, in response this finding, the Applications Development function opened POA&M 37055 with a planned completion date of July 1, 2021.

The source code security review identified medium-and low-risk security vulnerabilities

The IRM states that a code review shall be conducted for all new or modified systems going through a Security Assessment and Authorization that have not previously had a code review conducted and when code is being placed into production on an IRS information technology system. The IRS completed the required code review for the GMP application on April 3, 2020.

To satisfy NIST security controls requirement for Flaw Remediation and Information Input Validation (System and Information Integrity control family), the IRM[12] states that applications shall protect from cross-site scripting vulnerabilities, protect from command injection, and validate all input. In addition, the IRM also contains recommended best practices for logging and resource allocation. Our analysis of the source code security review report identified six security vulnerabilities (two medium risk and four low risk) related to input validation, injection, cross-site scripting, information leakage through log files, and improper resource shutdown due to using outdated software. All six of these vulnerabilities are associated with NIST security controls Flaw Remediation and Information Input Validation.

In addition, in the June 2020 GMP application's Security Assessment Report, the Cybersecurity function's Security Risk Management office issued a finding to the ICCE Authorizing Official stating that medium- and low-risk findings were identified in the Static Source Code Analysis and the Dependency Check Report. Failure to remediate all findings in the Source Code Analysis and the Dependency Check Report could result in known weaknesses in the application being exploited by malicious bad actors.

Management Action: On June 18, 2020, in response to this finding, the Applications Development function opened POA&M 37053 with a planned completion date of July 2, 2021.

The web application vulnerability report for the GMP application identified weak cryptographic ciphers

To satisfy the NIST security control requirement for Cryptographic Protection (System and Communications Protection control family), the IRM states that when cryptographic protection is used, IRS information systems shall use cryptographic modules that comply with applicable Federal laws, Executive Orders, directives, policies, regulations, and standards.

We requested a web application vulnerability report for the GMP application and on July 28, 2020, the IRS provided the January 2020 scan report. Based on our evaluation of the report, we found one medium-risk vulnerability due to the use of weak ciphers.

In addition, in the June 2020 GMP Security Assessment Report, the Cybersecurity function's Security Risk Management office issued a finding to the ICCE Authorizing Official stating that the web application scan had identified the use of weak ciphers. The use of weak cryptographic ciphers could be exploited by a malicious attacker and potentially compromise the system's confidentiality, integrity, and availability.

[12] IRM 10.8.6, *Information Technology Security, Application Security and Development* (July 21, 2020).

Management Action: On June 18, 2020, in response this finding, the Applications Development function opened POA&M 37054 with a planned completion date of July 1, 2021.

There is no Information System Component Inventory for the GMP application

To satisfy NIST security control requirement for Information System Component Inventory (Configuration Management control family), the IRM states that the IRS shall develop and document an inventory of information system components that accurately reflects the current information system. In addition, it should include all components within the authorization boundary of the information system and be at a level of detail necessary for tracking and reporting. Lastly, information system components shall be reviewed and updated at a minimum annually, and during system component installations, removals, and system updates.

During our review of the GMP application's Event-Driven Security Controls Assessment[13] and the GMP application's Security Assessment Report, we determined that the GMP application does not develop, maintain, or update an inventory for the GMP application that is at the required level of granularity and that contains all system components of the GMP application. When asked why the GMP application's inventory was not updated as required, officials from the Applications Development function stated that the inventory was not updated to include the GMP application because the ICCE Annual Security Controls Assessment had already started its review of the ICCE System Security Plan and the ICCE Information System Contingency Plan. Failing to develop, maintain, or update a complete inventory could result in information system components not being included in vulnerability and compliance scanning, as well as the information system contingency plan being inadequate if it is needed during an event.

Management Action: On June 18, 2020, in response to this deficiency, the Applications Development function opened POA&M 37052 with a planned completion date of July 1, 2021.

The Chief Information Officer should:

Recommendation 1: Ensure that critical and high security vulnerabilities are timely remediated based on agency-defined timelines.

Management's Response: The IRS agreed with the recommendation and will remediate the critical and high vulnerabilities identified in the audit.

Recommendation 2: Ensure that POA&Ms associated with the GMP application are completed timely based on agency defined timelines and processes.

Management's Response: The IRS agreed with the recommendation and will remediate the POA&Ms identified in the audit.

The Digital Identity Acceptance Statement Met Both Federal and Agency Security Requirements

In June 2017, the NIST updated technical requirements for Federal agencies related to authentication and identity risks associated with implementing digital identity services.[14]

[13] IRS, *Get My Payment Continuous Monitoring Assessment Plan* (May 21, 2020).
[14] NIST Special Publication 800-63-3, *Digital Identity Guidelines* (June 2017).

Federal agencies must perform risk assessments; select individual assurance levels for identity proofing, authentication, and federation (if applicable); determine which processes and technologies they will employ to meet each assurance level; and document these decisions in a Digital Identity Acceptance Statement.

The Digital Identity Acceptance Statement must include the assessed assurance levels, the implemented assurance levels, rationale if the implemented assurance levels differ from the assessed assurance levels, comparability demonstration of compensating controls, and rationale if federated entities are not accepted.

Agency procedures for the Digital Identity Risk Acceptance process implement the risk acceptance methodology required by the NIST.[15] Agency procedures also document the purpose, procedures, and outputs of each activity within the Digital Identity Risk Acceptance process and include three main components: assessment of assurance levels, assurance levels for implementation, and approval and oversight.

We reviewed the Digital Identity Acceptance Statement and all related documents for the GMP application. The IRS assessed the GMP application's appropriate identity and authenticator assurance levels at level two; however, the IRS implemented the GMP application's assurance levels at the less-restrictive level one. The NIST defines the components of level one and level two identity assurance and authenticator assurance as follows:

- Identity Assurance Level One: There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the authentication process are self-asserted or should be treated as such.
- Identity Assurance Level Two: Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. This level also introduces the need for either remote or physically present identity proofing.
- Authenticator Assurance Level One: Provides some assurance that the claimant controls an authenticator bound to the subscriber's account. This level requires either single-factor or multifactor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.
- Authenticator Assurance Level Two: Provides high confidence that the claimant controls authenticators bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocols. Approved cryptographic techniques are required at this level and above.

Although the IRS implemented identity and authenticator assurance levels that were below the assessed level, we found the Digital Identity Acceptance Statement met NIST and agency requirements by including a detailed implementation and rationale, compensating controls and risk mitigation factors, a description of risk acceptance, and a plan of action. Examples of the compensating controls and risk mitigation factors included providing passive protection against malicious bots, masking taxpayer bank account information except for the last four digits, limiting the number of daily attempts per Social Security Number, and sending audit records to the Cybersecurity function's Cyber Fraud Analytics and Monitoring team for review and

[15] IRS, *Digital Identity Risk Assessment* Standard Operating Procedures, Version 1.6 (July 2019).

detection of potential fraudulent activity. IRS officials reported that there were no confirmed cases of fraud in the GMP application associated with user's bank account information. In addition, due to the identification of potential high-risk transactions, the Cyber Fraud Analytics and Monitoring team recommended that 159,739 Economic Impact Payments be transitioned from direct deposit to paper check delivery.

By ensuring that the GMP application complies with all applicable NIST and agency security requirements related to digital identity services, the IRS properly implemented compensating controls to mitigate the risks from using inappropriate authentication controls, which could allow unauthorized access and activities, compromised taxpayer records, and lost revenue due to identity theft refund fraud.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to review the effectiveness of IRS systems security and operations related to the CARES Act Economic Impact Payment processing. To accomplish our objective, we:

- Interviewed key stakeholders within the Applications Development function and reviewed the results from our planning survey to determine the IRS tax systems involved in delivering the Economic Impact Payments to individual taxpayers.
- Analyzed IRS Information Alerts and interviewed key stakeholders from the Applications Development function to determine if any tax systems experienced a malfunction or performance issue specifically related to the implementation and delivery of the CARES Act legislation.
- Reviewed multiple security vulnerability reports, security assessment reports, risk assessment plans, a system security plan, and several POA&Ms to determine if the IRS implemented the GMP application's required baseline security controls and control enhancements established by the NIST and the IRM.
- Reviewed one security vulnerability report and two security assessment reports and conducted interviews with officials from the Applications Development and Cybersecurity functions to determine whether critical and high security vulnerabilities were timely remediated based on agency-defined timelines.
- Reviewed the Digital Identity Risk Assessment Determination, the Digital Identity Risk Assessment Ongoing Assessment, the Digital Identity Risk Assessment Tool Results, and Oversight and Pre-Oversight Voting Concurrence documents to determine whether the GMP application's Digital Identity Acceptance Statement met minimum Federal and agency security requirements.

Performance of This Review

This review was performed with information obtained from the Information Technology organization's Applications Development and Cybersecurity functions during the period April through October 2020. Due to the ongoing Coronavirus-19 pandemic, we conducted all audit work virtually. We held meetings and interviews via teleconference. We conducted this performance 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jena Whitley, Director; Jason McKnight, Audit Manager; Mike Curtis, Lead Auditor; Naomi Koehler, Senior Auditor; and Johnathan Elder, Information Technology Specialist (Data Analytics).

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: NIST requirements for selecting and specifying security controls for organizations and information systems supporting the Federal government and IRM polices related to information systems security requirements and the Digital Identity Risk Assessment and Acceptance process. We evaluated these controls by interviewing IRS employees and analyzing relevant documentation provided by the IRS.

Appendix II

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF INFORMATION OFFICER

MEMORANDUM FOR MICHAEL E. MCKENNEY,
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger
Acting, Chief Information Officer

Digitally signed by Nancy A. Sieger
Date: 2020.12.09 07:13:15 -05'00'

SUBJECT: Response to Draft Audit Report – Systems Processing Economic Impact Payments Performed Well and the Get My Payment Application Security Vulnerabilities Are Being Remediated (audit #202020626)

Thank you for the opportunity to review your draft audit report and to discuss observations with the audit team. The IRS response to the Coronavirus Aid, Relief, and Economic Security (CARES) Act was an enormous undertaking that produced overwhelmingly positive results.

We are on the front lines of implementing key economic COVID-19 relief, including helping taxpayers get their Economic Impact Payments as soon as possible. These payments are desperately needed by people hit by the aftermath of the coronavirus pandemic. IRS employees did what they always do – stepped up and delivered in this time of need to start the first round of these payments ahead of schedule. Working with the Treasury and the Bureau of Fiscal Services (BFS), IRS delivered a first tranche of payments totaling almost $150 billion for more than 80 million households only 14 days from passage of the CARES Act. Taxpayers started seeing the first Economic Impact Payments of $1,200 or more in bank accounts on April 15, which is usually Tax Day. Additional rounds of payments continued, ultimately helping more than 150 million Americans.

Simultaneously, IRS employees also delivered two special tools on IRS.gov to help taxpayers understand the law and provide millions of people who don't normally file a tax return a way to quickly register for these payments. There have been more than 200 million successful status checks on Get My Payment and more than 14 million people have successfully provided their banking information, meaning they received, or will receive, their payments much more quickly via direct deposit.

These complex undertakings, which occurred concurrently with the delivery of the 2020 filing season, required teams across the IRS to coordinate and decipher complex legislative requirements and identify the impact on tax processing systems. Additionally, the IRS worked cooperatively with the Social Security Administration, the Department of Veterans Affairs and other government agencies to pull more information into our systems to ensure that we could send payments to these groups of people without requiring them to file a return or take any other action.

Throughout this time and to protect the health and safety of taxpayers and IRS employees, the IRS rescaled operations by transitioning most of its employees to telework, hitting a record 59,000 simultaneous users. To further assist the public, we also implemented new coronavirus-related paid leave for workers and tax credits for small and midsize businesses to swiftly recover the cost of providing coronavirus-related leave in coordination with the Department of Labor.

We agree with TIGTA's two recommendations and will continue to ensure that critical and high security vulnerabilities are timely remediated. Our corrective action plan for the recommendations identified in the report is attached. The IRS is committed to meeting the needs of the American people in a safe and secure environment.

The IRS values TIGTA's continued support and assistance. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Robert E. Hill, Director, Applications Development, Delivery Management Quality Assurance, at (469) 801-0173.

Attachment

RECOMMENDATION #1: Ensure that critical and high security vulnerabilities are timely remediated based on agency-defined timelines.

CORRECTIVE ACTION #1: The IRS agrees with the recommendation and will remediate the critical and high vulnerabilities identified in the audit.

IMPLEMENTATION DATE : May 15, 2021

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Applications Development

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: Ensure that POA&Ms associated with the GMP Application are completed timely on agency defined timelines and processes.

CORRECTIVE ACTION #2: The IRS agrees with the recommendation and will remediate the POA&Ms identified in the audit.

IMPLEMENTATION DATE : August 15, 2021

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Applications Development

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

Appendix III

Glossary of Terms

Term	Definition
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Command Injection	An attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application.
Common Vulnerability Scoring System	Provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities. It attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.
Cross-site Scripting	A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client.
Cryptography (Cryptographic)	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.
Event-Driven Security Controls Assessment	Initiated when changes are made to an information system that affect security controls. This process only applies to Federal Information Security Modernization Act reportable information systems with an existing security authorization. It does not apply to new systems without a security authorization.
Exploit	Any method used by hackers to gain unauthorized access to computers, the act itself of a hacking attack, or a hole in a system's security that opens a system to an attack.
Hardening	A process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services.
Individual Master File	The IRS database that maintains transactions or records of individual tax accounts.
Information Leakage	The intentional or unintentional release of information to an untrusted environment.

Information System Contingency Plan	Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.
Input Validation	The proper testing of any input supplied by a user or application to prevent improperly formed data from entering an information system.
Moderate-Impact System	An information system in which at least one security objective (*i.e.*, confidentiality, integrity, or availability) is assigned a Federal Information Processing Standards potential impact value of moderate, and no security objective is assigned a potential impact value of high.
Multifactor Authentication	Using two or more different factors to achieve authentication. Factors include something you know (*e.g.*, password); something you have (*e.g.*, cryptographic device, token); or something you are (*e.g.*, biometric).
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Remediation	The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.
Security Assessment Report	Provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls.
Security Control	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Source Code	A set of instructions and statements written by a programmer using a computer programming language. This code is later translated into machine language by a compiler.
System Security Plan	A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
Vulnerability	A weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.
Weak Cipher	An encryption/decryption algorithm that uses a key of insufficient length.

Appendix IV

Abbreviations

CARES Act	Coronavirus Aid, Relief, and Economic Security Act
GMP	Get My Payment
ICCE	Integrated Customer Communications Environment
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones