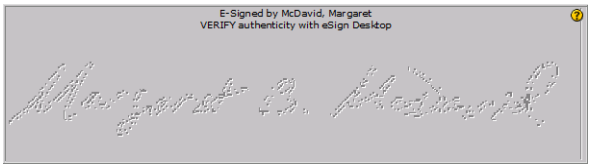
OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

July 27, 2020

MEMORANDUM FOR: GREGORY S. CRABB
VICE PRESIDENT, CHIEF INFORMATION SECURITY OFFICER

PRITHA N. MEHRA
VICE PRESIDENT, INFORMATION TECHNOLOGY



FROM: Margaret B. McDavid
Deputy Assistant Inspector General
for Inspection Service and Information Technology

SUBJECT: Management Alert – Risks Associated with Information Technology Applications (Report Number 20-251-R20)

This management alert presents risks associated with Information Technology (IT) applications developed under the [redacted]. These issues came to our attention during our ongoing audit of [redacted]. The objective of this management alert is to provide U.S. Postal Service officials immediate notification of the issues identified during our ongoing audit. The issues require immediate attention and remediation.

We identified these issues while conducting our 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.

We appreciate the cooperation and courtesies provided by your staff. If you have questions or need additional information, please contact Mary Lloyd, Director, Information Technology, or me at 703-248-2100.

Attachment

cc: Postmaster General
Vice President, Supply Management
Corporate Audit Response Management

Introduction

While conducting the [redacted], we found the Postal Service allowed IT applications to operate in the production environment with substantial vulnerabilities. Although the issues identified were not directly related to the scope of the audit, they are security weaknesses that warrant management's attention and corrective action.

The [redacted] was established to support Postal Service IT business operations and develop and maintain applications. Our objective is to inform the Postal Service of significant vulnerabilities associated with applications developed and maintained under this contract that did not complete the Certification and Accreditation (C&A) process.

Our fieldwork was planned before the President of the United States issued the national emergency declaration concerning the novel coronavirus disease outbreak (COVID-19) on March 13, 2020. The results of this alert do not reflect operational changes and/or service impacts that may have occurred as a result of the pandemic.

Conclusion

The Postal Service allowed applications to operate in the production environment with significant vulnerabilities that increase the risk of disclosure of sensitive information and potential impact to business operations.

Risks Associated with Applications Developed Under the [redacted]

The Postal Service allowed six of ten applications, four of the six which were sensitive,[1] to operate in the production environment with significant vulnerabilities. Specifically, the Corporate Information Security Office (CISO) allowed these applications to operate on the network for as long as seven years with incomplete C&As, such as missing risk acceptance letters,[2] risk mitigation plans,[3] approval signatures, and expired conditional[4] accreditation letters. In addition, they did not issue a *Failure to Comply* letter to the business owner when C&A requirements were not met.[5] The Postal Service did not completely evaluate the risks these vulnerable applications posed to Postal Service's IT environment.

---

[1] Additional security is required to adequately protect sensitive-enhanced, sensitive, and critical information resources. The level of protection must be based on the information's sensitivity. Sensitivity determines the need to protect the confidentiality and integrity of sensitive information.
[2] The Vice Presidents of IT and the functional business area accept responsibility for a documented vulnerability that will not be mitigated.
[3] Responsibility is assigned for the remediation and identify a remediation completion date.
[4] Requirements that need to be met within a certain time frame.
[5] *Handbook AS-805-A*, *Information Resource Certification and Accreditation (C&A) Process,* dated June, 2015. Section 4-6.4.12.

Postal Service policy[6] states that approvals, such as accreditation letters, are required before deploying an information resource. Additionally, if the requirements of the conditional accreditation letter are not met in the indicated timeframe, the accreditor[7] will issue a *Failure to Comply* letter to the Vice President of IT and the Vice President of the functional business area. Re-initiating the C&A process is required every one to three years.[8]

As a result, Postal Service applications operated in production with potential vulnerabilities which could lead to disclosure of sensitive data and unauthorized system access. Consequently, [redacted][9] last accreditation was in 2013 and it has been operating under an unapproved risk acceptance letter since 2018. We found 12 vulnerabilities related to [redacted] labeled as catastrophic by the CISO. Catastrophic vulnerabilities have a potential financial impact of over $1 billion.[10] These are common, well-known vulnerabilities that have been present for three years that could be exploited by an attacker utilizing publicly available methods.

This alert contains a summary of the completed and missing C&A documents for the ten applications we reviewed. We believe these issues require immediate attention and remediation (see Appendix A).

Recommendation #1: We recommend the **Vice President, Chief Information Security Officer**, in coordination with **Vice President, Information Technology**, complete the Certification and Accreditation process to evaluate the risk associated with the six applications with expired accreditations and mitigate or formally accept the risks.

Recommendation #2: We recommend the **Vice President, Chief Information Security Officer** issue a Failure to Comply letter if the conditional accreditation requirements for the six applications are not met.

Management's Comments

Management agreed with the finding and recommendations in the report. Regarding recommendation 1, management stated that they will provide all necessary certification

[6] *Handbook AS-805-A*, Section 4-8.4.2, *Deploy Information Resource*; Section 2-12, *Accreditor*; and Section 3-3, *Frequency of Certification and Accreditation*.
[7] Reviewing the risk mitigation plan and supporting C&A documentation package together with business requirements and relevant Postal Service issues.
[8] Re-initiating the C&A process for payment card industry information resources every year; sensitive-enhanced, sensitive, and critical information resources every two years; and all other information resources every three years.
[9] [redacted]
[10] According to the CISO's Impact Justification in the [redacted] Vulnerability Risk Ratings.

and accreditation documentation for the six applications with expired accreditations. The target implementation date is July 31, 2020.

Regarding recommendation 2, management stated that they will provide documentation for the six applications with expired accreditations. Additionally, they stated that upon providing accreditation letters to address recommendation 1, they will not issue Failure to Comply Letters. The target implementation date is July 31, 2020. See Appendix B for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations and corrective actions should resolve the issues identified in the report.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. All recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendix A: C&A Status of Applications Developed Under the [redacted]

	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Expired Accreditation						
1	[redacted]	Conditional	12.10.2013	6	2	RMP, RAL
2	[redacted]	Conditional	9.16.2013	6	2	Signature, RAL
3	[redacted]	Full	11.1.2013	6	2	None
4	[redacted]	Conditional	10.30.2013	6	2	RA, RMP, RAL
5	[redacted]	Conditional	12.22.2010	9	3	RA, RMP, RAL
6	[redacted]	Conditional	6.24.2009	10	3	RA, RMP, RAL
Current Accreditation						
7	[redacted]	Conditional	8.30.2019	0	2	None
8	[redacted]	Conditional	5.24.2019	0	2	None
9	[redacted]	Conditional	3.27.2018	1	2	Signature on AL
10	[redacted]	Full	2.20.2020	0	3	None

Notes: Risk Mitigation Plan (RMP), Risk Acceptance Letter (RAL), Risk Assessment (RA), Accreditation Letter (AL)
** Sensitive-Enhance and Sensitive applications require re-initiating C&A process every two years.
* Non-Sensitive applications require re-initiating C&A process every three years.
Source: CISO Cybersecurity Risk Management group, obtained February and May 2020.

Appendix B: Management's Comments

UNITED STATES POSTAL SERVICE

July 23, 2020

Lazerick C. Poland
Director, Audit Operations

SUBJECT: Management Alert – *Risks Associated with Information Technology Applications* (Project Number 20-251)

Thank you for the opportunity to review and comment on the Office of Inspector General (OIG) *Risks Associated with Information Technology* Applications – Management Alert. The United States Postal Service is dedicated to having a safe environment that protects sensitive information and prevents unauthorized system access. Management understands the intent of the draft report is to help improve and secure the production environment that allows applications to operate.

Overall, management agrees in the OIG's assessment of the current production environment and is immediately addressing the OIG's recommendations. CISO has implemented an update to its application accreditation process to a continuous monitoring approach which will ensure that these types of issues will not occur in the future.

Management is providing the following response to address the findings and recommendations cited in the *Risks Associated with Information Technology* Applications – Management Alert.

Recommendation [1]:
We recommend the **Vice President, Chief Information Security Officer**, in coordination with **Vice President, Information Technology**, complete the Certification and Accreditation process to evaluate the risk associated with the six applications with expired accreditations and mitigate or formally accept the risks.

Management Response/Action Plan:
Management agrees with this recommendation. CISO will provide all necessary Certification and Accreditation documents to the OIG for review, for risks associated with the six applications that previously held expired accreditations.

Target Implementation Date:
July 31, 2020

Responsible Official:
Vice President, Chief Information Security Office

Recommendation [2]:
We recommend the **Vice President, Chief Information Security Officer** issue a Failure to Comply letter if the conditional accreditation requirements for the six applications are not met.

Management Response/Action Plan:
Management agrees with this recommendation. CISO is working to provide the correct documentation to the OIG for review, for risks associated with the six applications that previously held expired accreditations. Upon providing the accreditation letters for Recommendation #1, CISO will have no Failure to Comply letters developed.

Target Implementation Date:
July 31, 2020

Responsible Official:
Vice President, Chief Information Security Office

Gregory Crabb

Digitally signed by Gregory Crabb
DN: cn=Gregory Crabb, o=US Postal Service, ou=Corporate Information Security Office, email=GSCrabb@uspis.gov, c=US
Date: 2020.07.22 16:42:08 -04'00'

Gregory S. Crabb
Vice President, Chief Information Security Officer

E-SIGNED by Pritha Mehra
on 2020-07-23 07:29:09 CDT

Pritha Mehra
Vice President, Information Technology