Description of document:	U.S. AbilityOne Commission (AbilityOne) Reports from two Inspector General (OIG) closed investigations 2017-2026
Requested date:	03-March-2025
Release date:	08-April-2026
Posted date:	20-April-2026
Source of document:	FOIA Administrator U.S. AbilityOne Commission 355 E Street SW Suite 325 Washington, D.C. 20024 Email: FOIA@abilityone.gov FOIA.gov

U.S. ABILITYONE COMMISSION

355 E Street SW, Suite 325
Washington, DC 20024

April 8, 2026

Reference: **FOIA- 2025-0026**

I am writing in response to your Freedom of Information Act (FOIA) request, dated March 3, 2025. Specifically, you requested in relevant part:

A copy of the final report, closing report, closing memo, report of investigation, referral memo, referral letter, or other conclusory document from these two OIG closed investigations: I18INV00037 Fraud opened 6/1/2018 closed 3/28/2024 AND I20INV00020 Fraud opened 1/13/2020 closed 3/28/2024.

The OIG's response to your request is as follows: The OIG has provided a copy of the final report, closing report, closing memo, report of investigation, referral memo, referral letter, or other conclusory document from OIG closed investigation I18INV0037 Fraud and I20INV0020.

In response to the request, please find the attached documents.
Redactions were made under FOIA exemption 5 U.S.C. § 522(b)(6), (b)(7)(c), and (b)(7)(e).

You have the right to appeal this response if you consider it to be a denial of your FOIA request (41 CFR 51-8.8). An appeal to the Committee Executive Director may be made by submission of a written request for reconsideration. Such requests shall state the specific reasons for reconsideration that addresses directly the ground upon which the denial was based and must be received at the Commission office within 90 calendar days of your receipt of this letter.

Sincerely,

Cassandra Assefa
Cassandra Assefa
U.S. AbilityOne Commission

UNITED STATES POSTAL SERVICE
OFFICE OF INSPECTOR GENERAL

Cyber Crimes Unit
Arlington, VA

CASE #: 21SPC01301 **CROSS REFERENCE #: N/A**

TITLE: Investigative Support to Ability One OIG

CASE AGENT (if different from prepared by): N/A

COMPUTER FORENSIC REPORT

PERIOD COVERED: FROM February 3, 2021 TO June 15, 2021

STATUS OF CASE: OPEN/CONTINUING INVESTIGATION

BACKGROUND

The U.S. Postal Service Office of Inspector General (USPS OIG) has a memorandum of understanding with AbilityOne OIG to provide digital forensic support.

REQUEST

AbilityOne OIG requested assistance determining if their Information Technology department circumvented technical measures that (b) (7)(C) during a Federal Information Security Modernization Act (FISMA) audit in 2019. Specifically, the allegation indicated the IT department enabled technical measures to (b) (7)(C) during the audit and subsequently disabled the after the audit was complete.

RELEVANT FINDINGS

AbilityOne utilized McAfee ePolicy Orchestrator (EPO) to manage endpoint security policies. Audit logs were exported from EPO which indicated numerous changes were made on October 17, 2019, that affected the (b) (7)(C) measures for a single computer. Additionally, the EPO Data Loss Prevention (DLP) Incident Manager reported 20 incidents related to a single computer (b) (7)(C).

The EPO DLP Policy Manager indicated the two policies that had the capability to [redacted] devices, "TEST" and "(b) (7)(C) [redacted]" policies, were not assigned to any systems at the time of the EPO virtual machine acquisition. These policies were last applied on October 17 and 31, 2019, respectively. Additionally, the "My Default DLP" policy was last applied on September 13, 2017, was assigned to five categories of systems, but did not contain any (b) (7)(C) [redacted] capability at the time of the virtual machine acquisition.

SUPPORTING DETAILS

Search Authority:

The (b)(6); (b)(7)(C) virtual machine was used and owned by AbilityOne. AbilityOne notifies its users via computer login banners that activity on AbilityOne systems may be monitored. SA (b)(6); reviewed the contents of the virtual machine's live Registry and noted the following key:

(b)(6); (b)(7)(C); (b)(7)(E)

contained the following information for the "legalnoticecaption" and "legalnoticetext" Registry values (Attachment 1):

> Notice to Users
>
> This is an official U.S. Government System for authorized use only. Use of this system constitutes consent to security testing and monitoring. Unauthorized use of this system or the information on this system could result in criminal prosecution. The information on this site is Predecisional for Official Use Only and cannot be disclosed outside of authorized individuals.

Items Examined:

1. Virtual machine, named "(b)(6); (b)(7)(C)

Acquisition Details:

On March 22, 2021, SA (b)(6); wrote a memorandum of activity documenting the acquisition and preservation of the (b)(6); (b)(7)(C) virtual machine (Attachment 2).

Analysis Details:

SA (b)(6), deployed the virtual machine template and gained access to the operating system by creating a "USPS" user account. (b)(6), (b)(7)(C) Network Engineer, U.S. AbilityOne Commission, assisted SA (b)(6), in creating a (b)(6), (b)(7)(C) account within EPO. Once logged in, SA (b)(6), exported an audit log and began exporting screenshots of EPO settings and incidents (Attachment 3 and Attachment 4, respectively).

Policy Structure

McAfee EPO used a hierarchal structure to distribute policies to endpoint systems. Policies can be applied to individual systems or groups of systems and consist of zero or more rule sets. Rule sets can consist of zero or more rules. Rules define a series of actions that should take place once certain criteria are met (Attachment 5).

Timeline

SA (b)(6), created the following timeline of events based off the EPO audit log and incidents:

Date/Time	Description	User/Computer
9/13/17 1:38:01 PM EDT	"My Default DLP Policy" policy created	(b)(6), (b)(7)(C)
9/13/17 1:38:01 PM EDT	Zero rule sets assigned to "My Default DLP Policy" policy	
4/3/18 2:06:24 PM EDT	"Test" rule created and applied to "prevect copy" rule set	
4/3/18 2:06:45 PM EDT	"prevect copy" rule set renamed "Test"	
4/3/18 2:07:39 PM EDT	"Test" rule set assigned to "test" policy	
4/3/18 2:08:51 PM EDT	"test" policy assigned to (b)(6), (b)(7)(C)	
4/3/18 2:11:45 PM EDT	"test" policy assigned to (b)(6), (b)(7)(C)	
4/3/18 2:17:57 PM EDT	[redacted]	
4/3/18 2:18:44 PM EDT		
4/3/18 2:23:09 PM EDT		

4/3/18 2:34:10 PM EDT	(b) (7)(C)	(b)(6); (b)(7)(C)
4/3/18 2:52:04 PM EDT	"test" policy assigned to (b)(6); (b)(7)(C)	
4/3/18 2:52:48 PM EDT	(b) (7)(C)	
4/3/18 2:52:48 PM EDT		
4/3/18 2:52:48 PM EDT		
4/3/18 2:52:48 PM EDT		
4/3/18 2:52:48 PM EDT		
4/3/18 2:52:48 PM EDT		
4/3/18 2:52:49 PM EDT		
4/3/18 2:55:02 PM EDT	"Test" rule set renamed to "(b) (7)(C) "	
4/3/18 2:55:30 PM EDT	"test" policy renamed to "(b) (7)(C) "	
4/3/18 2:55:31 PM EDT	"(b) (7)(C) " applied	
4/3/18 2:55:40 PM EDT	"(b) (7)(C) " rule set modified	
4/3/18 2:55:40 PM EDT	"(b) (7)(C) " policy modified	
4/3/18 2:55:42 PM EDT	"Test" rule of "(b) (7)(C) " rule set opened	
4/3/18 2:56:30 PM EDT	"(b) (7)(C) " rule set name changed to "AbilityOne DLP Rule set"	
4/3/18 2:56:30 PM EDT	"(b) (7)(C) " policy modified	
4/3/18 2:56:31 PM EDT	"Test" rule of "AbilityOne DLP Rule set" rule set opened	
4/3/18 2:56:49 PM EDT	"Test" rule name changed to "(b) (7)(C) "	

4/3/18 2:56:49 PM EDT	"AbilityOne DLP Rule set" rule set modified	(b)(6); (b)(7)(C)
4/3/18 2:56:49 PM EDT	"(b) (7)(C) [redacted]" policy modified	
4/3/18 2:57:33 PM EDT	USB device blocked	
4/3/18 3:00:04 PM EDT	"(b) (7)(C) [redacted] Policy" removed from (b)(6); (b)(7)(C)	
4/3/18 3:12:12 PM EDT	"(b) (7)(C) [redacted]" removed from (b)(6); (b)(7)(C)	
4/3/18 3:12:57 PM EDT	"(b) (7)(C) [redacted]" removed from (b)(6); (b)(7)(C)	
9/6/18 3:50:04 PM EDT	"My Default DLP Policy" policy copied to "My Default DLP Policy (copy)"	
9/6/18 3:50:07 PM EDT	Zero rule sets assigned to "My Default DLP Policy (copy)" policy	
9/6/18 3:50:07 PM EDT	"My Default DLP Policy (copy)" policy modified	
9/6/18 3:50:10 PM EDT	"My Default DLP Policy (copy)" policy applied	
10/17/19 11:01:01 AM EDT	Deployed McAfee agent	
10/17/19 11:01:02 AM EDT	(b)(6); (b)(7)(C) system added	
10/17/19 2:16:05 PM EDT	User "(b)(6); (b)(7)(C)" logged on	
10/17/19 2:32:16 PM EDT	"(b) (7)(C) [redacted]" rule of "AbilityOne DLP Rule set" rule set opened	
10/17/19 2:40:23 PM EDT	"(b) (7)(C) [redacted]" rule modified	
10/17/19 2:40:23 PM EDT	"AbilityOne DLP Rule set" rule set modified	

10/17/19 2:40:23 PM EDT	"(b) (7)(C) (b) (7)(C) " policy modified	(b)(6); (b)(7)(C)
10/17/19 2:41:49 PM EDT	"TEST RSD" rule created	
10/17/19 2:41:50 PM EDT	"AbilityOne DLP Rule set" rule set modified	
10/17/19 2:41:50 PM EDT	"(b) (7)(C) " policy modified	
10/17/19 2:43:18 PM EDT	"McAfee Default" policy copied to "TEST Policy"	
10/17/19 2:43:29 PM EDT	"TEST Policy" policy created	
10/17/19 2:43:29 PM EDT	Zero rule sets assigned to "TEST Policy" policy	
10/17/19 2:43:29 PM EDT	"TEST Policy" policy modified	
10/17/19 2:43:31 PM EDT	"TEST Policy" policy applied	
10/17/19 2:43:54 PM EDT	"TEST" rule set created	
10/17/19 2:44:17 PM EDT	"(b) (7)(C) " rule created	
10/17/19 2:44:17 PM EDT	"TEST" rule set modified	
10/17/19 2:44:25 PM EDT	"TEST RSD" rule created	
10/17/19 2:44:25 PM EDT	"TEST" rule set modified	
10/17/19 2:44:47 PM EDT	One rule set applied to "TEST Policy" policy	
10/17/19 2:45:00 PM EDT	"TEST Policy" policy applied	
10/17/19 2:51:43 PM EDT	"TEST Policy" policy assigned to (b)(6); (b)(7)(C) (b)(6); (b)(7)(C)	
10/17/19 1:53:26 PM CDT	(b) (7)(C)	
10/17/19 1:53:27 PM CDT	(b) (7)(C)	
10/17/19 1:53:59 PM CDT	(b) (7)(C)	
10/17/19 1:54:00 PM CDT	(b) (7)(C)	

		(b)(6); (b)(7)(C)
10/17/19 2:56:31 PM EDT	"(b) (7)(C) (b) (7)(C) " policy assigned to "My Organization"	
10/17/19 3:01:11 PM EDT	(b) (7)(C)	
10/17/19 3:04:29 PM EDT	(b) (7)(C)	
10/17/19 2:08:35 PM CDT	(b) (7)(C)	
10/17/19 2:08:35 PM CDT	(b) (7)(C)	
10/17/19 3:14:12 PM EDT	"My Default DLP Policy" policy assigned to "Workstations"	
10/17/19 3:14:32 PM EDT	"My Default DLP Policy" policy assigned to "Windows 10"	
10/17/19 3:14:46 PM EDT	"My Default DLP Policy" policy assigned to "Test Policy Window 10"	
10/17/19 3:15:02 PM EDT	"My Default DLP Policy" policy assigned to "My Organization"	
10/17/19 2:21:42 PM CDT	(b) (7)(C)	
10/17/19 2:21:42 PM CDT	(b) (7)(C)	
10/17/19 2:22:11 PM CDT	(b) (7)(C)	
10/17/19 2:22:46 PM CDT	(b) (7)(C)	
10/17/19 2:25:17 PM CDT	(b) (7)(C)	
10/17/19 2:25:17 PM CDT	(b) (7)(C)	
10/17/19 2:34:25 PM CDT	(b) (7)(C)	
10/17/19 2:35:25 PM CDT	(b) (7)(C)	

10/17/19 2:36:28 PM CDT	(b) (7)(C)	(b)(6); (b)(7)(C)
10/17/19 2:36:29 PM CDT	(b) (7)(C)	
10/17/19 2:43:06 PM CDT	(b) (7)(C)	
10/17/19 2:43:07 PM CDT	(b) (7)(C)	
10/17/19 3:44:55 PM EDT	User (b)(6); (b)(7)(C) logged off	
10/17/19 3:52:30 PM EDT	User (b)(6); (b)(7)(C) logged on	
10/17/19 3:53:02 PM EDT	"My Default DLP Policy" policy assigned to (b)(6); (b)(6); (b)(7)(C)	
10/17/19 4:22:54 PM EDT	User (b)(6); (b)(7)(C) logged off	
10/31/19 11:44:52 AM EDT	"My Default DLP Policy" policy assigned to "Windows 10"	
10/31/19 11:45:24 AM EDT	"(b) (7)(C) (b) (7)(C) " policy assigned to "Windows 10"	
10/31/19 11:45:35 AM EDT	"My Default DLP Policy" policy assigned to "Windows 10"	
10/31/19 12:45:05 PM EDT	"AbilityOne DLP Rule set (1)" rule set created	
10/31/19 12:45:06 PM EDT	"(b) (7)(C) (b) (7)(C) rule created	
10/31/19 12:45:06 PM EDT	"TEST RSD" rule created	
10/31/19 12:51:30 PM EDT	"(b) (7)(C) (b) (7)(C) policy modified	
10/31/19 12:51:39 PM EDT	"(b) (7)(C) (b) (7)(C) " policy applied	
10/31/19 1:14:59 PM EDT	"(b) (7)(C) (b) (7)(C) rule modified	

10/31/19 1:14:59 PM EDT	"TEST" rule set modified	(b)(6); (b)(7)(C)
10/31/19 1:14:59 PM EDT	"TEST Policy" policy modified	
10/31/19 2:00:14 PM EDT	"Test" rule modified	
10/31/19 2:00:14 PM EDT	"TEST" rule set modified	
10/31/19 2:00:14 PM EDT	"TEST Policy" policy modified	
10/31/19 2:00:26 PM EDT	"(b) (7)(C) " rule modified	
10/31/19 2:00:26 PM EDT	"TEST" rule set modified	
10/31/19 2:00:26 PM EDT	"TEST Policy" policy modified	
7/24/20 12:04:58 PM EDT	(b)(6); (b)(7)(C) moved to "Windows 10" group	

Summary

Based on the above timeline and the settings found in EPO, SA (b)(6); made the following observations:

1. The "My Default DLP Policy" policy was originally created on September 13, 2017 and did not contain any rule sets at any time during its existence.
2. On April 3, 2018, the "test" policy with the "Test" rule set with the "Test" rule" was assigned to the systems (b)(6); (b)(7)(C) and (b)(6); (b)(7)(C) Subsequently, 12 (b) (7)(C) incidents were reported to EPO for users (b)(6); and (b)(6); on the systems (b)(6); (b)(7)(C) " and (b)(6); (b)(7)(C) " This indicated the "Test" rule (later renamed "Block USB Storage Devices") of the "Test" rule set (later renamed "(b) (7)(C) " and "AbilityOne DLP Rule set") of the "test" policy (later renamed "(b) (7)(C) ") was effective at (b) (7)(C) devices. Subsequently, on the same day, the "(b) (7)(C) " policy assignment was removed from the three systems.
3. The "My Default DLP Policy" policy was copied to "My Default DLP Policy (copy)" on September 6, 2018. The new policy did not contain any rule sets at any time during its existence.
4. On October 17, 2019, the system (b)(6); (b)(7)(C) was added to EPO.
5. On October 17, 2019 at 2:16:05 PM EDT, the user (b)(6); (b)(7)(C) logged into EPO. During this session the following events took place:
   a. The "(b) (7)(C) " rule, "AbilityOne DLP Rule set" rule set, and "(b) (7)(C) " policy were modified.

b. A new "TEST Policy" policy with a new "TEST" rule set with a new "TEST RSD" was created. At 2:51:43 PM EDT, the "TEST Policy" policy was assigned to the system [redacted]. Four [redacted] incidents were reported to EPO for the user [redacted] on the system [redacted] which indicated the "TEST Policy" policy was effective at [redacted].
c. The "[redacted]" policy was assigned to the "My Organization" group. Two [redacted] incidents were reported to EPO for the user [redacted] on the system [redacted] and two [redacted] incidents were reported to EPO for the user [redacted] on the system [redacted]
d. The "My Default DLP Policy" was assigned to the groups "Workstations," Windows 10," "Test Policy Window 10," and "My Organization."
e. Twelve [redacted] incidents were reported to EPO for the user [redacted] on the system [redacted]
f. At 3:44:55 PM EDT, he user [redacted] logged out of EPO.

6. On October 17, 2019 at 3:53:02 PM EDT, the "My Default DLP Policy" policy was assigned to the system [redacted]
7. On October 31, 2019, several changes were made that affected the assignment and functionality of the "My Default DLP Policy," "[redacted]" and "TEST Policy" policies, the "AbilityOne DLP Rule set (1)" and "TEST" rule sets, and the "[redacted]," "TEST RSD," and "Test" rules.
8. The "[redacted]" appears to have been assigned to "My Organization" and "Windows 10" groups. However, the policy was not assigned to any groups at the time of the virtual machine acquisition. The logs do not indicate when or how the policy assignment was removed. SA [redacted] tested EPOs ability to purge select audit records. EPO had the ability to purge all records older than a certain date (e.g. one day, 30 days, one year, etc.). A new log entry was created for purged records.

Software Used:

VMware Workstation 15
McAfee ePolicy Orchestrator 5.3.2

Evidence Storage:

Western Digital USB hard drive, SN: [redacted]

ATTACHMENTS

1. AbilityOne login banner, May 26, 2021

AbilityOne banner.txt

2. Memorandum of Activity, March 22, 2021

MOA - Virtual machine transfer - 20:

3. McAfee EPO Audit log, May 24, 2021

EPO_Audit_Log_Entry.csv

4. McAfee EPO Screenshots, May 21, 2021

EPO Screenshots.pdf

5. McAfee EPO Help Pages for Rule Sets and Rules, May 26, 2021

McAfee Help Portal - Rule Sets.pdf

McAfee Help Portal - Rules.pdf

6/15/2021

X (b)(6); (b)(7)(C)

(b)(6); (b)(7)(C)
Special Agent
Signed by: (b)(6); (b)(7)(C)

PREPARED BY: (b)(6); (b)(7)(C)	DATE: 6/15/2021

Committee for Purchase From People Who Are Blind or Severely Disabled
(U.S. AbilityOne Commission)
Office of Inspector General

March 28, 2024

MEMORANDUM

TO: FILE

FROM: Steven N. Burke
Deputy Inspector General and
Assistant Inspector General for Investigations
Office of the Inspector General

DIG Steven N. Burke
cn=DIG Steven N. Burke, o=U.S. AbilityOne OIG, ou=Office of Inspector General, email=sburke@oig.abilityone.gov, c=US
2024.03.28 08:29:44 -04'00'
2023.008.20555

SUBJECT: Closure of Investigation # I 20INV00020

The U.S. AbilityOne Commission Office of the Inspector General (AbilityOne OIG) conducted an investigation into alleged employee misconduct to determine whether the U.S. AbilityOne Commission's (Commission) (b) (7)(C)(b) (7)(C)(b) (7)(C) directed federal contractors to manipulate the Commission's server policy settings and circumvent technical measures that block the (b) (7)(C) during the FY19 Federal Information Security Management Act (FISMA) audit and then instructed contractors to reenable (b) (7)(C) when the audit was completed. AbilityOne OIG entered a Memorandum of Understanding (MOU) with the United States Postal Service (USPS) OIG's cybercrimes unit for digital forensics support in analyzing the Commission's McAfee ePolicy Orchestrator (EPO).[1]

The OIGs were unable to substantiate the allegations as the McAfee EPO audit logs did not indicate when or how the [redacted] assignment was edited.[2] Additionally, the McAfee EPO Audit log showed no entries indicating a data purge occurred around the FISMA audit timeframe as to suggest

[1] McAfee ePolicy Orchestrator (ePO) is a centralized management and security console designed by McAfee, a cybersecurity company. It allows organizations to centrally manage and enforce security policies across their network, including antivirus protection, endpoint security, data encryption, and more. ePO provides administrators with visibility into their organization's security posture, the ability to deploy security updates, and to respond to security incidents efficiently.

[2] United States Postal Service Office of the Inspector General Cyber Crimes Unit, Report #21SPC01301 (Feb. 3, 2021 – June 15, 2021)

evidence was deleted.[3] AbilityOne OIG determined to close the investigation as unsubstantiated with no further action.

BACKGROUND:

Structure of IT Office

During the investigative timeframe, (b) (7)(C) (b) (7)(C) The IT office has historically experienced significant turnover among its contractors. From a risk-based perspective, the OIG noted that this structure introduced potential vulnerabilities in maintaining consistency, transfer of knowledge, and adherence to security protocols.

FISMA

The Federal Information Modernization Security Act (FISMA) requires OIGs to conduct an annual independent evaluation of its agency's information security program, practices, and controls. FISMA was enacted by Congress to ensure the security and integrity of public systems. The security of federal systems and data is essential to preventing data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information.

AbilityOne OIG engaged the independent public accounting firm (IPA) McConnell & Jones to conduct the annual evaluation and complete the fiscal year FY19 IG FISMA Reporting Metrics.[4] The objective of the evaluation was to assess the effectiveness of the Commission's security program and practices across key functional areas. On July 19, 2019, OIG sent a Notification Letter to the Commission that 2019 FISMA audit was beginning. The letter specified that audit would assess the effectiveness of the Commission's information security and privacy program from October 1, 2018, to September 30, 2019. An entrance conference was held on August 19, 2019. On August 27th, McConnell & Jones communicated selection of controls for testing. On September 9th, McConnell & Jones performed on-site physical testing/fieldwork.[5] From October 9th to October 10th,

[3] McAfee EPO Audit log, May 24, 2021.
[4] https://www.cisa.gov/sites/default/files/publications/fisma_metrics_v1.3_final_508c.pdf
[5] Evaluation of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act, Report No. 20-01, Scope and Methodology, 3 (specifying the security testing).

McConnell & Jones provided an issue discussion draft of the FISMA Metrics to Commission IT staff, and IT staff provided technical comments back on the draft. McConnell & Jones issued the final IG FISMA Metrics to OIG and IT staff on October 25th. On October 30th McConnell & Jones conducted an exit conference and issued a draft audit report to OIG. Commission IT management had until November 15th to provide comments on the draft audit report. On November 21, 2020, OIG published the final audit report along with a transmittal letter to the Commission.

INVESTIGATIVE ANALYSIS:

On November 19, 2020, AbilityOne OIG and USPS OIG interviewed (b) (7)(C) (b) (7)(C)(b) (7)(C) who informed that the (b) (7)(C) and another (b) (7)(C), to disable the (b) (7)(C) before the FISMA audit testing began and then to reauthorize (b) (7)(C) after FISMA testing ended.[6] (b) (7)(C) reportedly told (b) (7)(C) that (b) (7)(C) is supposed to be disabled, and remain disabled, from a (b) (7)(C); (b) (7)(C) described (b) (7)(C) as nonresponsive.[7] (b) (7)(C) (b) (7)(C) (b) (7)(C) disabled and re-enabled the (b) (7)(C).[8] (b) (7)(C) recalls IT providing screenshots of the various McAfee settings to the FISMA auditors, including the setting where (b) (7)(C) was disabled.[9]

On or around March 22, 2021, (b) (7)(C) helped the OIGs access and preserve a (b) (7)(C)(b) (7)(C)(b) (7)(C)(b) (7)(C) USPS OIG exported an audit log and began exporting screenshots of EPO settings and incidents.[10] USPS OIG determined the following:

1. The "My Default DLP Policy" policy was originally created on September 13, 2017, and did not contain any rule sets at any time during its existence.

https://www.oversight.gov/sites/default/files/oig-reports/21.a%20FY%202019%20FISMA%20Evaluation%2C%20Report%20No.%2020-01%20%28Public%20Report%29.pdf

[6] Memorandum of Interview, (b) (7)(C)(b) (7)(C), U.S. AbilityOne Commission (Nov. 19, 2020).

[7] *Id.*

[8] *Id.*

[9] *Id.*

[10] United States Postal Service Office of the Inspector General (b) (7)(C)(b) (7)(C)(b) (7)(C) (Feb. 3, 2021 – June 15, 2021) (referencing Exhibit 3 and 4 attached).

2. On April 3, 2018, the "test" policy with the "Test" rule set with the "Test" rule" was assigned to the systems (b) (7)(C) ." Subsequently, 12 USB blocking incidents were reported to EPO for users " and " on the systems (b) (7)(C) ." This indicated the "Test" rule (later renamed "(b) (7)(C) ") of the "Test" rule set (later renamed " " and "AbilityOne DLP Rule set") of the "test" policy (later renamed "(b) (7)(C) ") was effective at blocking (b) (7)(C). Subsequently, on the same day, the "(b) (7)(C) " policy assignment was removed from the three systems.

3. The "My Default DLP Policy" policy was copied to "My Default DLP Policy (copy)" on September 6, 2018. The new policy did not contain any rule sets at any time during its existence.

4. On October 17, 2019, the system (b) (7)(C) was added to EPO.

5. On October 17, 2019 at 2:16:05 PM EDT, the user " logged into EPO. During this session the following events took place:

   a. The "(b) (7)(C) " rule, "AbilityOne DLP Rule set" rule set, and "(b) (7)(C) " policy were modified.

   b. A new "TEST Policy" policy with a new "TEST" rule set with a new "TEST RSD" was created. At 2:51:43 PM EDT, the "TEST Policy" policy was assigned to the system (b) (7)(C) Four (b) (7)(C) incidents were reported to EPO for the user (b) (7)(C) on the system (b) (7)(C) " which indicated the "TEST Policy" policy was effective at (b) (7)(C) .

   c. The "(b) (7)(C) " policy was assigned to the "My Organization" group. Two (b) (7)(C) incidents were reported to EPO for the user (b) (7)(C) on the system (b) (7)(C) and two (b) (7)(C) incidents were reported to EPO for the user (b) (7)(C) on the system (b) (7)(C)

   d. The "My Default DLP Policy" was assigned to the groups "Workstations," Windows 10," "Test Policy Window 10," and "My Organization."

e. Twelve (b) (7)(C) incidents were reported to EPO for the user [redacted] on the system (b) (7)(C) [redacted]

f. At 3:44:55 PM EDT, he user "[redacted] logged out of EPO.

6. On October 17, 2019 at 3:53:02 PM EDT, the "My Default DLP Policy" policy was assigned to the system "(b) (7)(C) [redacted]

7. On October 31, 2019, several changes were made that affected the assignment and functionality of the "My Default DLP Policy," "(b) (7)(C) [redacted]," and "TEST Policy" policies, the "AbilityOne DLP Rule set (1)" and "TEST" rule sets, and the "(b) (7)(C) [redacted]," "TEST RSD," and "Test" rules.

8. The "(b) (7)(C) [redacted]" appears to have been assigned to "My Organization" and "Windows 10" groups. However, the policy was not assigned to any groups at the time of the virtual machine acquisition. The logs do not indicate when or how the policy assignment was removed. [redacted] tested EPOs ability to purge select audit records. EPO had the ability to purge all records older than a certain date (e.g. one day, 30 days, one year, etc.). A new log entry was created for purged records.

CONCLUSION:

AbilityOne OIG was unable to substantiate the allegations as the McAfee EPO did not indicate when or how the [redacted] assignment was edited.[11] Additionally, the McAfee EPO Audit log showed no entries indicating a data purge occurred during FISMA audit timeframe as to suggest evidence was deleted.[12] Therefore, AbilityOne OIG determined to close the investigation with no further action.

A detailed review of the records identified and reviewed in this investigation did not provide any additional evidence or information to warrant further investigation or presentation to the United States Attorney's Office.

[11] United States Postal Service Office of the Inspector General Cyber Crimes Unit, Report #21SPC01301 (Feb. 3, 2021 – June 15, 2021).
[12] McAfee EPO Audit log, May 24, 2021.

Committee for Purchase From People Who Are Blind or Severely Disabled (U.S. AbilityOne Commission) Office of Inspector General

Investigation # I 20INV00020 is now closed.

Committee for Purchase From People Who Are Blind or Severely Disabled (U.S. AbilityOne Commission) Office of Inspector General

March 28, 2024

MEMORANDUM

TO: FILE

FROM: Steven N. Burke
Deputy Inspector General and
Assistant Inspector General for Investigations
Office of the Inspector General

DIG Steven N. Burke
cn=DIG Steven N. Burke, o=U.S. AbilityOne OIG, ou=Office of Inspector General, email=sburke@oig.abilityone.gov, c=US
2024.03.28 08:28:18 -04'00'
2023.008.20555

SUBJECT: Closure of Allegation 18-37

The U.S. Attorney's Office for the Eastern District of Kentucky (USKYE) initiated an investigation into the AbilityOne non-profit agency (NPA) (b) (7)(C)(b) (7)(C)(b) (7)(C) [redacted] as part of a series of investigations into alleged AbilityOne Program fraud predating the establishment of the U.S. AbilityOne Commission Office of the Inspector General (AbilityOne OIG). After its inception, AbilityOne OIG joined the investigative team alongside Army Criminal Investigative Division (CID). The investigation sought to determine whether [redacted] falsified compliance with the Javits-Wagner-O'Day (JWOD) Act's 75% overall direct labor ratio (ODLR) by declaring employees severely disabled without an adequate medical evaluation or normal competitive employability assessment. Specifically, the investigation focused on whether [redacted] relied on disability diagnoses made by hired psychologists who [redacted] paid more to diagnose the prospective employee as severely disabled and on employability assessments conducted by [redacted] rehabilitation counselors who were never trained on the AbilityOne Program requirements.

The investigation revealed evidence suggesting that [redacted] hired at least three psychologists to make medical and employability determinations who were unaware of AbilityOne requirements and who were instructed to complete standardized [redacted] medical forms instead of individual medical letterhead.[1] The detail of the nature and extent of the condition on the standard forms differed from when employees presented medical records from [redacted] hired psychologists. Witnesses

[1] *See* (b) (7)(C)(b) (7)(C)(b) (7)(C)(b) (7)(C)(b) (7)(C)(b) (7)(C)(b) (7)(C)

testified that [redacted] paid the psychologist more for diagnosing someone as severely disabled than as not severely disabled. [redacted] also appears to have hired and counted individuals towards the 75% ODLR basing their disability diagnoses solely on their involvement in drug court.

The investigative team interviewed former employees, reviewed medical records, and hired an expert to review a sample of medical evaluations. The expert determined that: 84% of files lacked sufficient information available to make a disability determination; 81% of files did not list accurate functional limitations based on the employee's experience and diagnosed disability; and 78% of the files listed inappropriate accommodations for the employee; and 78% of the files did not properly determine that the employee was severely disabled and unable to maintain normal competitive employment.[2]

On January 14, 2021. USKYE hosted a settlement conference [redacted] with a continuing integrity agreement (CIA) to ensure adequate training of rehabilitation specialists. [redacted] declined the offer. In the summer of 2021, the AUSA traditioned off the case. USKYE assigned a new AUSA in summer of 2022. AbilityOne OIG briefed the new AUSA and sought to resume settlement discussions. However, new USKYE leadership and the new AUSA declined to move forward with the investigation citing statute of limitations issues and significant litigation risks to recover under the False Claims Act (FCA).

After receiving DOJ declinations, AbilityOne OIG has concluded to close the case with no further action.

Allegation 18-37 is now closed.

[2] *Id.*