TO: J. Christopher Giancarlo, Chairman
Brian D. Quintenz, Commissioner
Rostin Behnam, Commissioner
Dawn Stump, Commissioner
Dan M. Berkovitz, Commissioner

FROM: Miguel A. Castillo, *CPA, CRMA*
Assistant Inspector General for Auditing

DATE: May 13, 2019

SUBJECT: Briefing Report: Unaccounted Laptops

In September 2015, CFTC purchased 425 Dell 7450 laptops. In November 2018, CFTC management asked this Office to investigate 34 unaccounted laptops from that purchase; management feared they might be missing or stolen. We determined to have OIG audit staff initiate a review. Our goal was to assess internal controls for laptop accountability (safeguarding assets), ascertain the extent to which control failures (if any) might have played a role in the handling of the September 2015 purchase, and to make the proper referral if the facts indicated theft. We limited our scope to the September 2015 purchase.

To complete our review, we interviewed key personnel to gain an understanding of the information technology (IT) inventory process and the September 2015 purchase. We obtained and reviewed relevant documentation, inventory management policies related to IT assets, and Office of Financial Management cycle memos.

We conclude that current CFTC internal controls do not permit us to determine whether laptops were stolen or not, and that a full inventory must be performed to determine whether September 2015 laptops identified as unaccounted are in use or storage but not properly documented, or lost or stolen. In fact, during our fieldwork potential irregularities regarding laptop inventory tracking and documentation (from other shipments) came to light.[1] Given the present posture, we recommend that CFTC prioritize completion of a full inventory, and refer any indications of theft or fraud to OIG. In addition, internal controls should be enhanced in design and effectiveness to assure the reliability of IT inventory processes in the future. Given CFTC's reliance on contractors for IT asset management support, appropriate contract modifications in concert with policy updates may be necessary and are encouraged.

---

[1] These laptops were outside the scope of this review and we therefore can make no findings at this time.

Management Comments and Evaluation

We provided management a draft report for comments. We note management has acknowledged system shortfalls with its asset management system, has implemented short-term measures for controlling assets, and is migrating to a new asset management system to address gaps identified. Additionally, management is evaluating its contract pertaining to technology asset management to ensure it reflects CFTC needs.

Since our draft report, management has discovered several additional groups of missing laptops. In our eyes, the control environment has allowed for unauthorized removal of government property and changes to asset management records. We believe the short and long-term corrective actions will mitigate future losses.

Attached are our briefing report and management comments in its entirety. If you have any questions please call me at (202) 418-5084.

Cc:

Michael Gill, Chief of Staff

Kevin S. Webb, Chief of Staff

John Dunfee, Chief of Staff

Daniel Bucsa, Chief of Staff

Erik Remmler, Chief of Staff

Anthony C. Thompson, Executive Director

Daniel Davis, General Counsel

John Rogers, Chief Information Officer

A. Roy Lavik, Inspector General

Judith A. Ringle, Deputy Inspector General and Chief Counsel

Briefing Report: Unaccounted Assets

U.S. COMMODITY FUTURES TRADING COMMISSION
OFFICE OF THE INSPECTOR GENERAL

Background

Internal Control

Internal controls set out the plans, methods, policies, and procedures to help managers achieve desired results through effective stewardship of public resources. An internal control system is a continuous built-in component of operations, effected by people, that provides reasonable assurance, not absolute assurance, that an entity's objectives will be achieved.
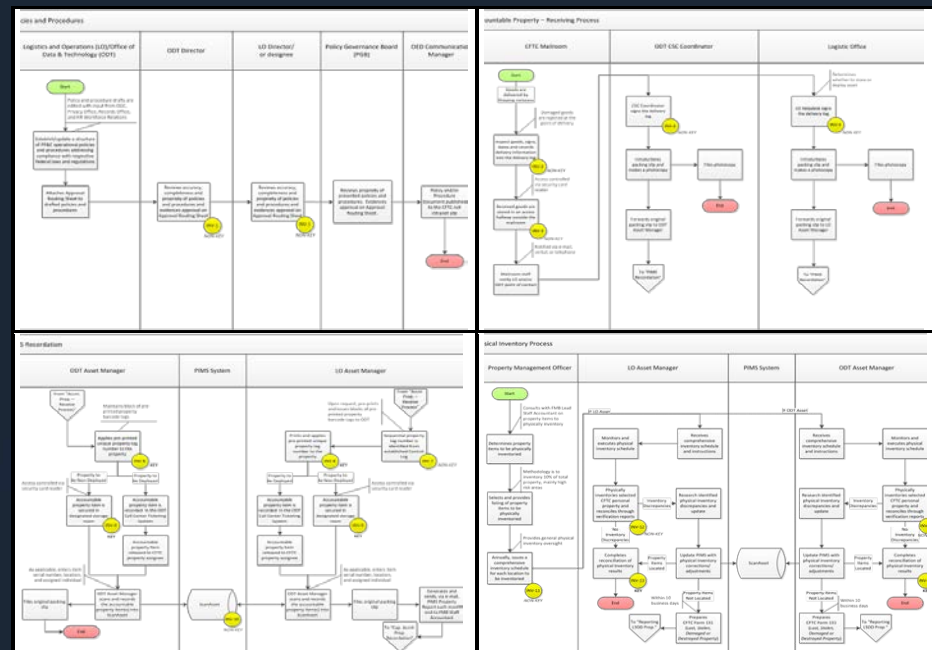
Safeguarding of Assets

Management designs an internal control system to provide reasonable assurance regarding prevention or prompt detection and correction of unauthorized acquisition, use, or disposition of an entity's assets.

Operating Effectiveness

In evaluating operating effectiveness, management determines if controls were applied at relevant times during the period under evaluation, the consistency with which they were applied, and by whom or by what means they were applied.

Background – CFTC Inventory Controls

- CFTC has controls in place for inventory.

- Key controls include processes for acceptance, recordation, periodic physical inventory, and loss reporting. Physical inventory is set at 10% of total property, mainly high risk areas, and considers value.

- Internal control reviews and independent audits have reported non-material weaknesses for inventory.

Source: Financial Management Office. _Inventoriable Assets Cycle Memo_

Objective and Scope

Our objective was to evaluate controls in place for IT equipment accountability (safeguarding assets).

Our scope was limited to a CFTC September 2015 purchase of 425 Dell 7450 laptops and reported losses from that purchase.

What We Did

To complete our review, we interviewed key personnel to gain an understanding of the information technology (IT) inventory process. We obtained and reviewed relevant documentation and procedures related to safeguarding IT equipment, as well as the Property Inventory Management System (PIMS), and CFTC financial management controls. In reference to laptop losses, we reviewed receiving reports, the associated contracts, and available system data.

What We Observed

- CFTC has adequate acceptance controls for reportable assets which in this instance worked as designed. While we did not find instances where assets were lost at acceptance, we noted tagging occurred about 3 weeks after acceptance. Timely tagging of laptops increases accountability of these assets.

- CFTC's PIMS procedures are outdated with asset management responsibility assigned to a CFTC officer no longer in existence ("OMO Asset Manager").

- PIMS does require weekly reviews of assets that are not assigned to any location. This review ensures that assets are assigned in a reasonable period of time. For unaccounted assets this did <u>not</u> occur after the initial scan.

What We Observed (cont.)

- ScanAsset is an archaic system for tracking information technology equipment. ODT staff reported system glitches impacting record completeness, including laptop assignment and location; however, CFTC is moving to a new system (ServiceNow) this year.

- PIMS does not assign responsibility for completeness of location information in ScanAsset. The Catapult contract (_Core Infrastructure Operations and Maintenance and Support Services_) is explicit for asset management requirements including record completeness. We believe it is incumbent upon the COR to ensure the completeness of system records.

- While Catapult contract terms are detailed for inventory management and loss processes, given the magnitude of unaccounted laptops, we conclude there is an overall weakness that exists for ensuring execution of contract terms and monitoring.

What We Observed (cont.)

- Lastly, we noted that ODT has no detailed procedures for issuing reportable assets to end users and updating ScanAsset. Such procedures can be used as a basis for monitoring contract compliance.

What We Suggest

To improve the prevention or prompt detection and correction of unauthorized acquisition of CFTC laptops:

1. We suggest CFTC Management :

   - Update PIMS and follow accordingly. Some improvement ideas provided during this review include:
     - Setting a timeframe for tagging after vendor delivery and CFTC acceptance,
     - Reviewing badge scans of secure rooms on a weekly basis to detect unauthorized personnel or unusual entry times, and
     - Installing security cameras in the storage rooms for incident reference.

What We Suggest (cont.)

2. We also suggest ODT management:
   - Establish procedures for issuing reportable assets to assigned users.
   - Review systems logs to verify information is accurate and complete and to detect unusual update activity .
   - Ensure that Catapult asset management contract terms are fully executed and monitored or modify accordingly.

Conclusion

We feel that in order for ODT to find all of the unaccounted laptops under the scope of our review, a full inventory must be done. Management conveyed that before CFTC migrates from ScanAsset to ServiceNow, a full inventory will be conducted.

MANAGEMENT COMMENTS

U.S. Commodity Futures Trading Commission
Three Lafayette Centre, 1155 21st Street, NW, Washington, DC 20581

Anthony C. Thompson
OED Executive Director

202-418-5697
athompson@cftc.gov

MEMORANDUM

To: A. Roy Lavik, Inspector General

From: Anthony C. Thompson, Executive Director

Date: April 23, 2019

Subject: Management response to OIG Briefing Report: Unaccounted Laptops

Thank you for the opportunity to respond to the suggestions in the OIG Briefing Report: Unaccounted Laptops. When we began the process of procuring and deploying a new asset management system, we discovered the apparent disappearance of a significant number of laptops. We asked the OIG to investigate. The OIG decided to do a limited audit that examined only one group of laptops that the agency had identified as missing.

During the course of the limited audit, and while the agency prepared for the deployment of the new asset management system, the agency discovered several additional groups of missing laptops, set forth in Appendix A. Throughout the audit, agency staff informed OIG staff of any additional missing laptops discovered.

The OIG's first suggestion is to update the agency's asset management system. We whole-heartedly agree. Asset management is of paramount importance to the CFTC, and although agency staff works tirelessly to manage thousands of assets within its control, a solid asset management solution is important for a successful asset management program. We have witnessed the inconsistencies with our current asset management system, ScanAsset, first-hand. We have experienced staff entering data into ScanAsset, logging out of the system and then logging back into the system only to discover that the previous data that had been entered was not captured by ScanAsset. We have implemented a verification process to ensure that the data is captured until the new replacement asset management system is online. The new asset management system, Service Now, will address many of the gaps we have identified in our current asset management program.

While the CFTC currently has policies and processes concerning its asset management program, there have been times where breakdowns have occurred and errors made. In an effort to mitigate and improve the physical handling of the assets, process gaps identified have been accounted for and staff has been retrained on the proper execution of the policies and procedures. The CFTC ODT IT Customer Support Center (CSC) work instruction for asset handling has been updated in an effort to ensure all assets removed from rooms 0306 and 0324 are documented by requiring a completed new Asset Acknowledgement Form prior to removing an asset from storage rooms. The CSC now also performs a weekly audit of all assets checked out of the storage rooms, and weekly badging reports are provided to ODT from OED Physical Security in an effort to audit the traffic in and out of the storage rooms. The badging reports are reviewed by the COR, the Alt COR, and Catapult Management (the contractor providing support for the program). Finally, access to storage rooms 0306 and 0324 has been limited to a small, necessary group of individuals.

Additionally, we are working to ensure that the language in the contract pertaining to asset management is reflective of the needs of the CFTC. The COR will ensure the appropriate monitoring is executed and consistent with the terms of the contract.

All of these mitigation steps were things that the CFTC had identified and was in the process of implementing before this report was issued. Due to resource constraints, we have not previously been able to perform a complete, comprehensive review of all assets within our inventory and have had to make do with partial inventories or spot inventories. However, we are pleased to report that as part of the deployment of the Service Now system, we will be doing a 100% inventory. Unfortunately, we still have a number of missing laptops, as noted above, that we cannot account for, and thus we again reached out to the OIG to determine whether the disappearance of these assets was the result of theft or fraud. While we were disappointed that the OIG initially decided to undertake only a review of the situation, it is our understanding that there is now an ongoing investigation into this matter. We look forward to assisting the OIG with the investigation.

In conclusion, we appreciate the ongoing work of the IG's Office in conducting this review and the pending investigation as we work to further implement the suggestions and improve the process and handling of the CFTC's IT assets.

2

Appendix A

- Group A: 1 missing based on shipment (2017)

- Group B: 36 Dell Latitude 7450 (2016)

- Group C: 1 Dell Latitude 7470 (2017)

- Group D: 3 Dell Latitude 7470 (Lost in shipping) (2018)

- Group E: 10 missing discovered via audit (2019)

- Group F: 10 Asset serial number changes in ScanAsset (2018)

- Group G: 2 additional 7470 Laptops discovered missing (2019)

3