Audit Report

OIG-07-035

BILL AND COIN MANUFACTURING: Control Weaknesses Need To Be Addressed at BEP's Western Currency Facility

March 30, 2007

Office of Inspector General

Department of the Treasury

Contents

Contents

Abbreviations

BEP	Bureau of Engraving and Printing
Bureau	Bureau of Engraving and Printing
CCTV	Closed Circuit Television
COPE	Currency Overprinting, Examining, and Packaging Section
GAO	Government Accountability Office
Mut Schedule	BEP Product Accountability System Schedule of Delivery of Mutilated Paper
OIG	Office of Inspector General
PSS	Product Security Station
SVS	Securities Verification Section
WCF	Western Currency Facility

March 30, 2007

Larry R. Felix
Director
Bureau of Engraving and Printing

The Bureau of Engraving and Printing (BEP) prints billions of Federal Reserve Notes for delivery to the Federal Reserve System each year. These notes are produced at the Washington, DC, facility and at the Western Currency Facility (WCF), which is located in Fort Worth, Texas. In October 2004, a WCF employee removed at least $5,000 of $50 Federal Reserve Notes slated for destruction.

The overall objectives of our audit were to determine the internal control failures at WCF that allowed the theft to be perpetrated and to determine whether BEP enhanced internal controls to (1) prevent the occurrence of a similar theft and (2) provide for timely detection should another theft occur.

To address our objectives, we reviewed BEP policies and procedures, product accountability control system print-outs, and security incident reports. We also reviewed external reports, and internal BEP reports and memoranda.

We made two visits to WCF, during which we conducted walk-throughs of the currency production floor and observed production activities. We observed the verification, [1]

[1] The term *verification* refers to a detailed process that includes ensuring that mutilated currency is accurately counted and properly defaced. In this report, this term refers to the final complete count prior to destruction.

authentication,[2] and destruction of mutilated currency, and reviewed related documentation. We also discussed controls with WCF management, conducted interviews, and followed up on the recommendations in an interim report[3] that we issued after our first onsite visit. A more detailed description of our objectives, scope, and methodology is provided in appendix 1.

Results in Brief

We concluded that the reason the October 2004 theft was able to be perpetrated was due not to an absence of internal control so much as to a failure to follow existing controls. In addition, while BEP has taken corrective actions to address issues identified following the theft, additional steps should be taken to enhance internal controls.

One of the major factors in the theft was the violation of existing policies and procedures, rather than the lack of internal control in this area. Specifically, an employee providing relief for one of the final verifiers in the Securities Verification Section (SVS) cage[4] handled mutilated currency even though such action was expressly prohibited by policies and procedures. Since the theft was discovered, management has instituted a more-restrictive policy, requiring that the SVS operation be shut down whenever a verifier needs a break instead of bringing in relief personnel.

Another factor that could help prevent the occurrence of a similar theft, or provide for timely detection, is improving the camera coverage. At the time of the October 2004 theft,

[2] *Authentication*, as currently used, refers to the random spot-checking of verified mutilated currency by [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

[3] *BILL AND COIN MANUFACTURING: Control Issues Identified at the Bureau of Engraving and Printing Western Currency Facility*, OIG-06-015 (Dec. 8, 2005).

[4] In this report, the term *SVS cage* refers to the location in the Currency Overprinting, Examining, and Packaging section where verification occurs.

policies and procedures did not require constant, live viewing by the Product Security Station (PSS) staff for activities occurring in highly vulnerable areas. This requirement was subsequently added.

During our audit, we found that policies and procedures were not followed in some instances and that noncompliance had been identified by both internal and external reviews of WCF operations, but had not been adequately addressed.

We are concerned about the absence of guidance for handling discrepancies in verification and authentication, including which unit(s) will assume custody and conduct an investigation. This is of particular importance because the October 2004 theft occurred in the SVS cage during verification and current procedures for authentication were implemented as a result of the theft. Further, we believe that the current procedures for authentication do not meet management's internal control objectives regarding the safeguarding of assets and do not allow for appropriate segregation of duties.

We also found that the bureau's tracking and accountability document for mutilated currency was not reflective of policies and procedures. As currently designed, the document does not provide adequate tracking and accountability information because it is not structured to require appropriate signatures by all employees involved at each of the control points determined by management. We also found that some forms were not fully completed.

Finally, we found that management has taken action to address the recommendations in our interim report by preparing a contingency plan, by ensuring that proper accountability was maintained over stored mutilated currency, and by requiring that it be verified before it was destroyed.

We are making six recommendations to the BEP Director to address the issues identified in this report. Specifically, the Director should ensure that (1) WCF supervisors ensure through monitoring and enforcement that WCF staff and contractor employees adhere

to policies and procedures; [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)] (3) clear, written policies and procedures are established that specify assignment of responsibility and actions to be taken if a discrepancy is found during verification or authentication; (4) the effectiveness of the authentication process is reevaluated; (5) personnel other than product security specialists are assigned to handle mutilated currency during authentication should it be decided to continue this process; and (6) tracking and accountability documents are modified to correspond to policies and procedures identifying each control point, and that these documents are completed as required.

In its response to our draft report, BEP management concurred with our recommendations. WCF employees are being held accountable for failure to adhere to policies and procedures and controls have been increased. A planned contract amendment will ensure that at least two persons are constantly monitoring the CCTV consoles. BEP also plans to reevaluate the current authentication process and has recently implemented a pilot program to explore changing the verification and authentication process at the WCF. The pilot program, according to BEP, reduces the number of times mutilated currency is handled, provides for a 100 percent verification, and maintains a clear chain of custody through to destruction. In conjunction with the pilot program, BEP plans to identify written policies and procedures that specify the assignment of responsibility and actions to be taken when discrepancies are found during the verification and authentication process. A final decision regarding the new approach is expected by July 2007, by which time tracking and accountability documents will also be modified.

We believe that the actions taken or planned by BEP address the intent of the recommendations. The text of the management response is included as Appendix 5.

Background

This section contains a brief description of WCF organizational units that were the focus of our audit.

The Currency Overprinting, Examining, and Packaging (COPE) Section prints seals and serial numbers on examined blank engraved sheets,[5] cuts the sheets into individual notes, examines the notes one final time, and initiates the preliminary packaging of the notes in preparation for final packaging prior to being issued to the Federal Reserve Banks.

The SVS performs onsite verification of mutilated currency[6] from various stages of the production process. SVS personnel review, verify, and sign schedules bearing the product identification and quantities of mutilated currency transferred to destruction. In addition, SVS personnel maintain accountability records, and develop and maintain verification and accountability procedures.

The Product Security Branch is a component of the Security Division and its primary function is to conduct internal investigations of alleged losses of bureau securities. Product security specialists provide the core of security expertise within the bureau and the substantive knowledge base upon which all bureau security programs and policies are built. In addition to investigative responsibilities, product security specialists assist with the implementation of physical security measures, including evaluating camera placement and field of view, and also oversee the destruction of mutilated currency.

Custody of mutilated currency that has been verified is transferred to the Product Security Branch for authentication. Once authentication is performed in the SVS section by two product

[5] These sheets of 16 subjects, which do not yet contain seals or serial numbers, have been through a mechanical examination process for quality control.
[6] The term *mutilated currency* refers to spoilage created during the production process. Although considered spoiled, some mutilated currency can be passed without nonexperts being able to detect that it is mutilated.

security specialists from this branch, the mutilated currency is transported to the destruction cage. Two printing plant workers assigned from the production sections to the destruction process are responsible for operating the destruction equipment, including loading the mutilated currency onto it.

The WCF Management Control Branch is responsible for maintaining comprehensive accountability oversight for all securities being manufactured and stored at the WCF. It administers and directs the implementation and monitoring of product accountability control systems and procedures to ensure the integrity of WCF securities. The Bureau of Engraving and Printing Management Information System, which includes the Product Accountability System, is the official system used to track manufacturing and accountability information.

Findings and Recommendations

Finding 1 Policies and Procedures Were Not Followed

We found that policies and procedures were not followed in some instances. This included policies and procedures that were in effect at the time of the October 2004 theft, as well as those instituted in response to it.

As described in *Standards for Internal Control in the Federal Government*,[7] a positive control environment is the foundation for all other standards. It provides discipline and structure as well as the climate which influences the quality of internal control. Agency management plays a key role in providing leadership in this area, especially in setting and maintaining the organization's ethical tone, providing guidance for proper behavior, removing temptations for unethical behavior, and providing discipline when appropriate.

[7] Issued by the Government Accountability Office (GAO) pursuant to the Federal Managers' Financial Integrity Act of 1982, the internal control standards for the federal government are prescribed in GAO publication GAO/AIMD-00-21.3.1, November 1999.

Failure to follow policies and procedures is an issue that has been previously identified by both internal and external reviews of WCF operations, but had not been addressed (appendix 3 contains excerpts from these reviews). [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

It was one of the issues reported in December 2000 as a result of an internal review of accountability, internal control, and operating procedures at the WCF.[8] This report also stated that "Bureau approved manuals, memorandums, and procedures had not been adhered to resulting in seven (7) recommendations for improvement," providing some indication of the general extent of noncompliance with policies and procedures at the WCF.

Failure to follow policies and procedures was raised again during external reviews by a contractor in October 2001 and August 2005 reports dealing with internal control.[9] As discussed below, we also observed during our viewing of recorded camera coverage that product security specialists were distracted during the destruction of mutilated currency.

Thus, vulnerabilities that existed, were identified, and should have been addressed, continued to exist because policies and procedures had not been enforced. Specifically, supervisors and managers may not have been monitoring the work of their respective units for compliance with, or may not have been enforcing, BEP policies and procedures. The circular titled *Bureau of Engraving and Printing Zero Tolerance Policy*[10] indicates that this

[8] [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

[9] [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

[10] [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

may have been the case when it refers to an "unofficial practice" that has been allowed over time of [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552(b)(2)]. In addition, an internal control review identified the need to refocus supervisory efforts away from custodial activities to monitoring and evaluation of the work of subordinates.

[REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

This is a highly vulnerable area designated by BEP as requiring dual control,[11] which means that access is to be accomplished by two authorized employees who during the course of their duties are required to be present and able to observe each other's activities at all times. In addition, all employees are required to be alert and aware of each other's activities, and to be within line of sight of each other at all times while in these areas.

We viewed recorded camera coverage of mutilated currency being destroyed at the WCF. We viewed tapes for the destruction processes that occurred on 8 days during the first two quarters of fiscal year 2006. In these recordings, we observed that the product security specialists did not comply with internal policies and procedures that require employees to be alert and aware of each other's activities and to be within line of sight of each other at all times.[12]

[11] [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

[12] [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

Specifically, we observed that the product security specialists were involved in activities other than overseeing the destruction process and that removed them from the line of sight of the printing plant workers who were destroying the mutilated currency. For example, the product security specialists were:

- completing paper work;
- preparing skids (reloading and moving the lift);
- walking away and leaving the view of the shredder;
- sweeping the caged area; and
- folding straps used to secure loads of mutilated currency sheets.

Additionally, we observed a failure by WCF personnel to follow two policies and procedures that were implemented in response to the October 2004 theft. We observed these conditions during both our site visits at WCF.

- Line of Sight Not Maintained in SVS Cage The two final verifiers working in the SVS cage, a dual control area,[13] did not adhere to the line of sight requirement; i.e., that all employees are required to be within line of sight of each other at all times while in these areas.

  This line of sight requirement had been instituted as a result of the October 2004 theft. Management told us that the intent was for the final verifiers to be facing each other while they worked. The SVS final verifiers that we interviewed confirmed that the policy requirement that they face each other had been conveyed to them by management.

  During our first onsite visit, we saw two final verifiers working in the SVS cage; one had his back turned to the other. During our second visit, we observed two final verifiers performing part

[13] [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

of a verification in the SVS cage, with the SVS Assistant Supervisor present. The two final verifiers were counting mutilated currency sheets side-by-side, which violated management's intent for the line of sight requirement.

These failures to follow policy occurred even though management had redesigned the work space to facilitate compliance.[14]

- CCTV Consoles Were Not Continuously Monitored By Two Persons We observed instances where only one contractor employee[15] was monitoring the CCTV consoles in the PSS. These consoles display views of security cameras on the production floor.

  CCTV cameras placed on the production floor are monitored by contractor employees in the PSS. Management stated that the cameras in the PSS are monitored by two contractors 24 hours/day, 7 days/week, 365 days/year, except some holidays. In addition, following the October 2004 theft, management implemented and verbally conveyed to the staff new policies and procedures that required notification to the PSS prior to the start of activities in highly vulnerable areas,[16] to ensure that constant, live viewing of the activities can occur. One purpose of live viewing is to detect suspicious behavior or security violations as they occur.

  During our onsite visits, we observed numerous instances where only one person was monitoring the CCTV consoles in the PSS, including one instance when only one contractor employee was monitoring the consoles while verification was occurring in the SVS cage. We believe that vulnerability

[14] [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

[15] We are not distinguishing between contractor employees who work at the WCF and BEP WCF employees when addressing issues dealing with policies and procedures.

[16] According to management, examples of highly vulnerable areas include destruction, final verification in the SVS cage, and shipping/receiving.

increases when only one person is monitoring all cameras in the PSS, especially during periods of activity in highly vulnerable areas. Constant attention to a highly vulnerable area leaves all other cameras without coverage. Conversely, if a single individual devotes attention to other cameras, inappropriate or suspicious behavior in a highly vulnerable area could go undetected.

Although we were told by WCF management that the policy was to have two persons monitoring the consoles in the PSS, the contract is not written to meet that requirement,[17] in part because, in addition to monitoring and recording CCTV video, contractor employees are required to perform other duties during their normal tour of duty. While under the terms of the contract two individuals are required to be on duty, it is not possible for both individuals to remain in the PSS monitoring the cameras on a constant basis given the other duties assigned as well as the need for breaks.

As management mentioned to us, it is just as important to have live coverage as to have the ability to subsequently view recorded activity. Had there been improved camera coverage at the time the October 2004 theft occurred, the theft may have been detected as it occurred.

The failure to ensure compliance with policies and procedures is an issue that needs to be addressed by WCF management. We note that in a memorandum dated May 3, 2005,[18] the BEP Director restated the BEP policy regarding responsibility for security, accountability, and safety of personnel and property. He emphasized that, "Under Bureau policy, section supervisors

[17] The contract states that:
The BEP requires a minimum of two individuals 24 hours/day, 7 days/week, 365 days/year to monitor, review, record, and operate routine activities as defined by the Product Security Branch Standard Operating Procedure. The center will be a continuous operation and shall not be unattended for lunch breaks, restroom breaks, or other activities.

[18] [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

have the responsibility and authority to take the necessary actions to protect and safeguard people, equipment, and production. Specifically, supervisors are responsible for monitoring the work activities of their staff as well as the activities of individuals in the area on official business to ensure that security and accountability policies and procedures are followed. The Director further stated that anyone who knowingly circumvents the established security, accountability, or safety controls, or allows or permits these controls to be circumvented, will be subject to the appropriate disciplinary action, up to and/or including removal."

Recommendations

We recommend that the BEP Director direct WCF management to do the following:

1. Ensure that WCF supervisors ensure through monitoring and enforcement that WCF staff and contractor employees adhere to policies and procedures.

   Management Comments

   BEP concurs. WCF employees are being held accountable when they fail to adhere to their policies and procedures; however, no action will ensure 100 percent compliance. Effective January 2007, WCF management has taken action by increasing the compensating controls by conducting additional unannounced compliance reviews, camera coverage reviews, and physical inventories.

   OIG Comment

   We believe that increased accountability and reviews focused on adherence to policies and procedures address the intent of the recommendation.

2. Ensure that two persons constantly monitor the CCTV consoles.

Management Comments

BEP concurs. By July 2007, the contract will be amended to ensure that at least two persons are constantly monitoring the CCTV consoles.

OIG Comment

We believe that the action planned by BEP addresses the intent of the recommendation.

Finding 2 Policies and Procedures Related to Discrepancies Found During Verification or Authentication Did Not Exist or Were Not Sufficiently Specific

We found that policies and procedures did not exist or were not sufficiently specific for the critical activities of mutilated currency verification and authentication.

According to *Standards for Internal Control in the Federal Government*, internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. The documentation should appear in management directives, administrative policies, or operating manuals and may be in paper or electronic form. All documentation and records should be properly managed and maintained.

During our audit, we found that policies and procedures did not exist for actions to be taken if a discrepancy is identified during the verification process. As noted earlier, the October 2004 theft occurred in the SVS cage during verification.

We also found that policies and procedures were not sufficiently specific with respect to actions to be taken if a discrepancy is

identified during authentication. Specifically, we found that current policies and procedures do not specify which unit will assume custody or conduct an investigation in such a case, and state only that "any discrepancies will be immediately reported to the Manager, Management Controls Branch and Manager, Product Security Branch." Although WCF management told us that other security personnel, such as WCF police officers, could be asked to conduct an investigation, no specific written policies and procedures exist that address the situation.

It is important that WCF management have a specific plan in place because the product security specialists – who have investigative training and responsibilities – would be precluded from conducting an investigation because, under current procedures, they handle mutilated currency during the authentication process. Using product security specialists to conduct an investigation of an authentication discrepancy would violate the principle of segregation of duties.

The absence of clear policies and procedures for handling discrepancies in verification and authentication could hinder investigation of such discrepancies.

Recommendation

1. We recommend that the BEP Director ensure that WCF management establishes clear, written policies and procedures that specify assignment of responsibility and actions to be taken if a discrepancy is found during verification or authentication. See our discussion regarding authentication in Finding 3. This recommendation applies to authentication only if management decides to continue this process.

   Management Comments

   BEP is reevaluating the current authentication process and in conjunction with the pilot program discussed under Finding 3, BEP plans to identify written policies and procedures that

specify the assignment of responsibility and actions to be taken when discrepancies are found during the verification and authentication process.

OIG Comment

We believe that the actions taken or planned by BEP address the intent of the recommendation.

Finding 3 Current Authentication Procedures Do Not Meet Internal Control Objectives and Do Not Allow for Appropriate Segregation of Duties

The current procedures for authenticating mutilated currency do not meet management's control objectives regarding the safeguarding of assets and do not allow for appropriate segregation of duties. [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

As discussed in *Standards for Internal Control in the Federal Government*, an agency must establish physical control to secure and safeguard vulnerable assets. Examples include security for and limited access to assets such as cash, securities, inventories, and equipment which might be vulnerable to risk of loss or unauthorized use. *Standards for Internal Control in the Federal Government* also states that key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. This should include separating the responsibilities for authorizing transactions, processing and recording them, reviewing the transactions, and handling any related assets. No one individual should control all key aspects of a transaction or event.

Because vulnerability increases each time mutilated currency is handled, this procedure may not be meeting management's control objectives. Further, we believe that when product security

specialists handle mutilated currency while performing random spot-checks after verification, duties are not properly segregated, which results in increased risk. In fact, to us it does not seem advisable to have product security specialists handling mutilated currency at any stage in the process, given their security roles and responsibilities.

Under current procedures, product security specialists are required to handle mutilated currency during authentication. This is of particular concern not only because their responsibilities include evaluating camera placement and field of view,[19] but also because product security specialists are experts trained to identify security vulnerabilities, and by the nature of their jobs know how vulnerabilities can be exploited.

Should an investigation into missing mutilated currency be warranted, these experts would not be able to participate in the investigation. As WCF management mentioned, other security personnel (e.g., police officers) could be asked to conduct the investigation; but we believe that those employees specifically trained to investigate such incidents should be the ones to conduct the very investigations they were specially trained to perform.

Recommendations

We recommend that the BEP Director do the following:

1. Reevaluate the effectiveness of the current authentication process and, in doing so, consider the objectives for these procedures in safeguarding assets, as well as the potential risks associated with these procedures.

[19] [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

2. Assign personnel other than product security specialists to handle mutilated currency during authentication should it be decided to continue this process.

Management Comments

BEP concurs to reevaluate the current authentication process and has implemented a pilot program to explore changing the verification and authentication process for COPE mutilated work at the WCF. The pilot program reduces the number of times mutilated currency is handled, provides for a 100 percent verification, and maintains a clear chain of custody from COPE through the verification to destruction. A final decision regarding the new approach is expected by July 2007.

OIG Comment

It should be noted that under the pilot program described by BEP, product security specialists do not handle mutilated currency during the verification and authentication process. We believe that the actions taken and planned by BEP address the intent of the recommendations.

Finding 4 Tracking and Accountability Documents Are Not Compatible With Policies and Procedures

BEP's tracking and accountability document for mutilated currency, the BEP Product Accountability System Schedule of Delivery of Mutilated Paper – also referred to as a Mut Schedule – was not reflective of policies and procedures or the actual process for the transfer of mutilated currency from COPE to SVS to destruction. We also found that some forms were not fully completed. A sample of the Mut Schedule is included as appendix 4.

As stated in *Standards for Internal Control in the Federal Government,* control activities should be effective and efficient in accomplishing the agency's control objectives. Yet the

Mut Schedule, as currently designed, does not provide adequate tracking and accountability information. Without properly designed and properly completed Mut Schedules, mutilated currency cannot be effectively tracked and accounted for.

We found that the Mut Schedule was not structured to require appropriate signatures by all employees involved at each of the control points determined by management. Although WCF policies and procedures are not as specific as they should be, we found that staff were not following the policies and procedures, in part, because the form was not structured in a manner to permit compliance. For example, policies and procedures stated that the Mut Schedule was to be signed and dated by the final verifiers. The final verifiers, who report to SVS, are assigned to work in teams of two. The corresponding section on the Mut Schedule states, "I/We hereby certify that the stock listed in this schedule has been verified by us," but only one signature line is provided and it is designated for the "receiving component signature," not the final verifiers.

In addition, we found that some of the forms were not fully completed. For example, in a number of instances, including the form in appendix 4, the section "Additional personnel assigned to the Destruction cage for destruction during this timeframe: …" was not completed. Management told us that the section was added so all individuals, including WCF printing plant workers, involved with the destruction process would be identified by signing the Mut Schedule.

For the reasons discussed above, in case of a discrepancy, management cannot tell by looking at the Mut Schedules who was involved in each step of the process. [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

Recommendation

1. We recommend that the BEP Director ensure that tracking and accountability documents are modified to correspond to policies and procedures identifying each control point, and that these documents are completed as required.

   Management Comments

   BEP concurs. Tracking and accountability documents will be modified by July 2007. In addition, a Request for Information Services has been generated to modify the wording on the Mut Schedules and to incorporate the change procedure for verification and authentication.

   OIG Comment

   We believe that the actions taken or planned by BEP address the intent of the recommendation.

Finding 5 Management Has Taken Action to Address Recommendations in OIG Interim Report

BEP has taken corrective action to address the two recommendations made in our December 2005 interim report,[20] in which we reported that (1) WCF did not have a contingency plan for destroying mutilated currency during periods when its destruction equipment was not functioning and (2) the mutilated currency that was being stored was vulnerable to theft.

One of our two recommendations was that BEP develop and implement contingency plans at WCF to provide for the destruction of mutilated currency in a timely manner when WCF destruction equipment is not functioning. In response, WCF management prepared "Western Currency Facility, Security Division, Destruction

[20] OIG-06-015.

Contingency Plan."[21] [REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

We also recommended that the BEP Director should, with respect to the mutilated currency that had accumulated, ensure that proper accountability was maintained and require that the stored mutilated currency be verified before destruction. In its response to our report, management stated that BEP had verified approximately 36 percent of the mutilated currency straps and then destroyed all of the straps by November 23, 2005. In addition, management said that BEP inspected individual skids and verified seals before transferring the mutilated currency to the destruction cage. The entire backlog of mutilated currency was destroyed by December 2, 2005.

During our visit to WCF in February and March 2006, we reviewed the Mut Schedules documenting the verification of the mutilated currency straps. Specifically, we reviewed a total of 27 Mut Schedules for the 8,146 straps that were verified prior to destruction. Because our review occurred subsequent to destruction, we could not reconcile actual inventory to the Mut Schedules. According to WCF management, the straps were destroyed and no exceptions were identified.

[21] The contingency plan was dated February 28, 2006, and was signed by the Acting Manager, Security Division, and by the Manager, Facilities Management Division, on that date. The document was signed again on March 8, 2006, by the same officials, without revision to the date on the front of the document. While the text of the plan itself remained essentially the same, the content of one of the appendices was significantly revised.

* * * * * * *

We appreciate the courtesies and cooperation provided to our staff. If you wish to discuss this report, you may contact me at (202) 927-5746 or Maria V. Carmona, Audit Manager, at (202) 927-6345. Major contributors to this report were Ms. Carmona; Susan R. Sebert, Analyst-In-Charge; Horace A. Bryan, Auditor; and Gabriel Ortiz, Special Agent.

John F. Lemen
Acting Director, Fiscal Service Audits

The overall objectives of our audit were to determine the internal control failures at the Bureau of Engraving and Printing's (BEP) Western Currency Facility (WCF) that allowed the October 2004 theft to be perpetrated and to determine whether BEP enhanced internal controls to (1) prevent the occurrence of a similar theft and (2) provide for timely detection should another theft occur.

To address these objectives, we reviewed BEP policies and procedures, including, but not limited to, those excerpted in appendix 2. We reviewed product accountability control system (Bureau of Engraving and Printing Management Information System) print-outs. We also considered WCF security incident reports. We reviewed external reports and internal BEP reports and memoranda, including, but not limited to, those listed in appendix 3.

We made two onsite visits to WCF; the first from October 31 through November 4, 2005, and the second from February 27 through March 2, 2006. During these visits, we conducted walk-throughs of the currency production floor and observed production activities and the operation of the Product Security Station. We observed the verification, authentication, and destruction of mutilated currency. We reviewed, for completeness and compliance with policies and procedures, documentation related to these processes, including the BEP Product Accountability System Schedules of Delivery of Mutilated Paper. This included review of documentation for dates for which we viewed recorded closed-circuit television coverage and for dates on which closed-circuit television coverage confirmed that the employee who perpetrated the October 2004 theft was in the Securities Verification Section cage.

We also discussed controls with WCF management, and conducted interviews as appropriate. In addition, we followed up on the corrective actions that BEP outlined in its response to the

recommendations in an interim report that we issued on some of the results of our first onsite visit.[22]

We conducted our audit in accordance with generally accepted government auditing standards.

[22] *BILL AND COIN MANUFACTURING: Control Issues Identified at the Bureau of Engraving and Printing Western Currency Facility*, OIG-06-015 (Dec. 8, 2005).

[REDACTED AT BEP'S REQUEST PURSUANT TO TREASURY FOIA REGULATION 31 C.F.R. § 1.5(c)(3)]

[REDACTED AT BEP'S REQUEST PURSUANT TO
TREASURY FOIA REGULATION 31 C.F.R. § 1.5(c)(3)]

[REDACTED AT BEP'S REQUEST PURSUANT TO TREASURY FOIA REGULATION 31 C.F.R. § 1.5(c)(3)]

[23]

[23] [REDACTED AT BEP'S REQUEST PURSUANT TO TREASURY FOIA REGULATION 31 C.F.R. § 1.5(c)(3)]

[REDACTED AT BEP'S REQUEST PURSUANT TO TREASURY FOIA REGULATION 31 C.F.R. § 1.5(c)(3)]]

[REDACTED AT BEP'S REQUEST PURSUANT TO TREASURY FOIA REGULATION 31 C.F.R. § 1.5(c)(3)]

[REDACTED AT BEP'S REQUEST PURSUANT TO TREASURY FOIA REGULATION 31 C.F.R. § 1.5(c)(3)]

[REDACTED AT BEP'S REQUEST PURSUANT TO TREASURY FOIA REGULATION 31 C.F.R. § 1.5(c)(3)]

[REDACTED AT BEP'S REQUEST PURSUANT TO TREASURY FOIA REGULATION 31 C.F.R. § 1.5(c)(3)]

[REDACTED AT BEP'S REQUEST PURSUANT TO TREASURY FOIA REGULATION 31 C.F.R. § 1.5(c)(3)]

[REDACTED AT BEP'S REQUEST PURSUANT TO TREASURY FOIA REGULATION 31 C.F.R. § 1.5(c)(3)]

[REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

[REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

.

[REDACTED – FOIA EXEMPTION 2, 5 U.S.C.§552 (b)(2)]

DEPARTMENT OF THE TREASURY
BUREAU OF ENGRAVING AND PRINTING
WASHINGTON, D.C. 20228

March 30, 2007

MEMORANDUM FOR JOHN F. LEMEN, ACTING DIRECTOR
OFFICE OF FISCAL SERVICE AUDITS
OFFICE OF INSPECTOR GENERAL

FROM: Leonard R. Olijar
Chief Financial Officer

SUBJECT: Draft Audit Report – Review of Internal Controls at the Western Currency Facility

Thank you for the opportunity to review the Office of Inspector's General's (OIG) draft audit report "Review of Internal Controls at the Western Currency Facility." The Bureau of Engraving and Printing (BEP) offers the following comments on the draft report.

Finding 1, Recommendation 1:

Ensure that WCF supervisors ensure through monitoring and enforcement that WCF staff and contractor employees adhere to policies and procedures.

Comment:

BEP concurs with this recommendation. WCF employees are being held accountable when they fail to adhere to their policies and procedures; however, no action will ensure 100 percent compliance. Effective January 2007, WCF Management has taken action by increasing the compensating controls by conducting additional unannounced compliance reviews, camera coverage reviews, and physical inventories.

Finding 1, Recommendation 2:

Ensure that there are two persons constantly monitoring the Closed Circuit Television (CCTV) consoles.

Comment:

BEP concurs with this recommendation and by July 2007 the contract will be amended to ensure that at least two persons are constantly monitoring the CCTV consoles.

Finding 2, Recommendation 1:

We recommend that the BEP Director ensure that WCF management establishes clear, written policies and procedures that specify assignment of responsibility and actions to be taken if a discrepancy is found during verification or authentication.

Comment:

BEP concurs to reevaluate the current authentication process and in conjunction with the pilot program discussed under Finding 3 will identify written polices and procedures that specify the assignment of responsibility and actions to be taken when discrepancies are found during the verification and authentication process.

Finding 3

Recommendation 1:

We recommend that the BEP Director reevaluate the effectiveness of the current authentication process and, in doing so, consider the objectives for these procedures in safeguarding assets, as well as the potential risks associated with these procedures.

Recommendation 2:

We recommend that the BEP Director assign personnel other than product security specialists to perform authentication should it be decided to continue this process.

Comment:

BEP concurs to reevaluate the current authentication process and has implemented a pilot program to explore changing the verification and authentication process for COPE mutilated work at the WCF. The pilot program reduces the number of times muts are handled, provides for a 100 percent verification, and maintains a clear chain of custody from COPE through the verification to destruction. A final decision regarding the new approach is expected by July 2007.

Finding 4, Recommendation 1:

We recommend that the BEP Director ensure that tracking and accountability documents are modified to correspond to policies and procedures identifying each control point, and that these documents are completed as required.

Comment:

BEP concurs with this recommendation. Tracking and accountability documents will be modified by July 2007. In addition, a Request for Information Services (RIS) has been generated to modify the wording on the mut schedules and to incorporate the change procedure for verification and authentication.

Department of the Treasury

Office of Strategic Planning and Performance Management
Office of Accounting and Internal Control

Bureau of Engraving and Printing

Director
Associate Director (Chief Financial Officer)

Office of Management and Budget

OIG Budget Examiner