

Supplement

System Administration Tool- SAT Security Best Practices

January, 2009
Document Version 1.0

Change/Revision History

Date	Section/Chapter	Revision/Change Description	Page/Section Affected
01/2009		Original Citibank Release	

Table of Contents

Glossary of Acronyms	4
Purpose	5
What is P I I?.....	5
Secondary Storage	5
Access Control	6
Risk Assessment.....	8
Personnel Security and Procedures.....	9
Physical and Environmental Protection	11
Contingency Planning.....	13
Configuration Management.....	15
System Maintenance	16
System and Information Integrity	17
Media Protection	19
Incident Response.....	21
Awareness and Training.....	22

Glossary of Acronyms

CFR – Code of Federal Regulations

ELVIS - **E**lectronic **V**erification **I**maging **S**ystem. ELVIS is the host application where all check images are stored.

FIPS – Federal Information Processing Standards

FISMA – Federal Information Security Management Act

FRB-C – Federal Reserve Bank of Cleveland

NIST – National Institute of Standards and Technology

OMB – Office of Management and Budget

PCC OTC – Paper Check Conversion Over the Counter

PII – Personally Identifiable Information

POC – Point of Contact. The person who has access to the SAT (System Administration Tool) and can add/delete/update users in the POS, or make configuration changes in the SAT.

POS – Point Of Sale. A component is the PCC OTC system. The POS is the PC-based software to capture images of the check along with transaction data.

SAT – System Administration Tool. A module used in the POS system for setting up and managing system security and configuration.

USB – Universal Serial Bus is a connection port on a computer that is universally compatible with many types of devices, such as, printers, speakers, mouse, flash drives, etc. Can support speeds of up to 12Mbps.

PCC OTC Security Best Practices

Purpose

The document was written to provide security best practices for the PCC OTC system that will guide agencies toward FISMA (Federal Information Security Management Act) compliance. This document outlines points from the *NIST Special Publication 800-53*. Each Agency's internal guidelines should take Treasury security best practices into consideration. Please refer to *NIST Special Publication 800-53* for complete text of the 'Recommended Security Controls for Federal Information Systems'.

What is P I I?

Personally Identifiable Information (P I I) is information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history. It includes information which can be used to distinguish or trace an individual's identity such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc (*OMB M-06-19 (July 12, 2006)*).

PCC OTC Batch information contains PII information. It is therefore critical that this data be secured to prevent unauthorized access to this highly sensitive information.

Secondary Storage

PCC OTC requires the use of a secondary storage device. This device is used to retain batch information and check images in the event of a computer failure or data corruption on the hard drive prior to transmission. The number of days that the data is stored on the storage device is configured within the SAT of the POS computer. The PCC OTC secondary storage device could be in the form of a folder on a LAN drive, a smartcard, a zip disk or a USB flash drive. Without the secondary storage, daily processing information would not be retained and would not be available for transmission or batch recovery in the event of a computer failure.

Special precautions are necessary in order to safeguard the sensitive information that is stored on the secondary storage drive, especially if that storage drive is in the form of a USB flash drive, smartcard, zip disk or other compact storage device. These small, external media types are very compact and easy to lose or steal. The POS provides a minimum level of encryption to the data stored on the secondary storage drive which may prevent unauthorized users to read the data. Agencies may also consider using additional levels of encryption to protect the data on the secondary storage drive. This can be accomplished by purchasing software that is specifically designed to encrypt data on removable media. (If encryption of stored information is employed as an access enforcement mechanism, the cryptography used must be FIPS 140-2 compliant. For additional information, see section SC-13 of the *NIST Special Publication 800-53*.) If additional levels of encryption are used, agencies must ensure that the data can be de-encrypted for use in the event that the data needs to be restored using the POS 'Batch Recover' function. De-encryption will typically involve the use of a password. If the additional level of encryption cannot be removed, the POS will be unable to read the batch data and the batch recovery function will fail. Contact your Information Technology staff to obtain more information.

Access Control

N I S T Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented access control policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal documented procedures to facilitate the implementation of the access control policy and associated risk assessment controls¹.

Effects on PCC OTC

- ❖ Agencies must identify authorized users of PCC OTC and specify access rights/privileges. Access is granted to PCC OTC based on a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria and intended system usage. Agencies must monitor and remove unnecessary access when users are terminated or transferred and associated accounts need to be removed, or when a user's access changes.
- ❖ Agencies enforce separation of duties through assigned access authorizations by establishing appropriate divisions of responsibility and separates duties as needed, to eliminate conflicts of interest in the responsibilities and duties of individuals who have access to the PCC OTC system.
- ❖ Agencies employ the concept of least privilege for specific duties.
- ❖ Agencies enforce a limit of consecutive invalid access attempts by a user. This limit should be no more than three attempts.
- ❖ Agencies must review audit records, i.e., activity logs, of the PCC OTC system for inappropriate activities in accordance with organizational procedures. Agencies must investigate any unusual information system-related activities and periodically review change to access authorizations. N I S T Special Publication 800-92 provides guidance on computer security log management.

In Summary

- Access to the PCC OTC should be given to users at the lowest level available that still allow the user to perform their job duties. For information on POS and ELVIS roles and permissions, please refer to the *SAT* chapter of the *PCC OTC User Manual*, 'User Administration' section, and the *ELVIS* chapter of the *PCC OTC User Manual*, 'What is PCC OTC?' section.
- Review separation of duties for users performing tasks on the POS computer. For example, users that key in batch information should not have access to the SAT to add or edit users, or make changes to configurations settings. Separation of duty can be taken a step further by assigning permission to perform voids, batch close/transmission, and batch input to different individuals.
- Ensure that the maximum number of failed login attempts to the POS computer has not been altered to a number higher than 3. For complete instructions, please refer to the *SAT* chapter of the *PCC OTC User Manual*, 'System Configuration' section.

¹ This process should be documented within the agency's User Manual.

- Review and certify POS users yearly. FMS performs annual certification of users for the ELVIS system. Local procedures should be established for performing recertification of POS users on each POS computer. PCC OTC Point of Contact should print out a listing of users and their associated roles/permissions in the SAT and re-evaluate their POS job responsibilities. Complete instructions for printing this list can be found in the *SAT* chapter of the *PCC OTC User Manual*, 'User Administration' section.

Risk Assessment

N I S T Special Publication 800-53 Guidance

Agency develops, disseminates, and periodically reviews/updates:

1. A formal documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Effects on PCC OTC

Risk assessment identifies risk through a formal process and makes a conscious decision to accept, mitigate, or avoid that risk. Agencies can request a Business Risk Assessment template that will assist them in their risk assessment of the PCC OTC system in their environment. To request the template, contact the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 4, option 5, option 4 or via email at FMS.OTCChannel@citi.com.

Also, refer to *FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems*, which can be used to categorize and measure risk of information and information systems.

Personnel Security and Procedures

N I S T Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal documented procedures to facilitate the implementation of the personnel security policy and associated personnel security policy and procedure controls.

Effects on PCC OTC

- ❖ Assign a risk designation to all positions and establish screening criteria for individuals filling those positions. (*N I S T Special Publication 800-12 and 5 CFR 731.106(a) and Office of Personnel Management policy and guidance*).
- ❖ Screen individuals requiring access to the PCC OTC system and PCC OTC information before authorizing access. (*5 CFR 731.106(a) and Office of Personnel Management policy, regulations, and guidance; organizational policy, regulations and guidance; FIPS 201 and Special Publication 800-73 and 800-76; and the criteria established for the risk designation of the assigned position*)
- ❖ Ensures completion of the appropriate access agreements, i.e., Rules of Behavior, Privacy Statement, Accessibility Statement, and all information security access forms for individuals requiring access to PCC OTC before authorizing access.
- ❖ Establish personnel security requirements for third-party providers, i.e., service bureaus, contractors, and other organizations providing PCC OTC information technology services or network management, and monitor the provider to ensure adequate security. (*N I S T Special Publication 800-35*).
- ❖ Establish a formal disciplinary process for individuals that blatantly disregard security procedures.. The process can be included as part of the general personnel policies and procedures.
- ❖ When employment is terminated, or individuals are reassigned or transferred to other positions within the agency, terminate access to the PCC OTC system and to PCC OTC information (both the POS and ELVIS), ensure the return of all PCC OTC related property, i.e., printouts, flash drives used as secondary storage, etc., and ensure that the appropriate personnel have access to official records created by the terminated employee that are stored on the PCC OTC system or paper files.

In Summary

- Assign a risk category or designation to all positions associated to the PCC OTC system and screen individuals before granting access to the system.
- Make certain users read and understand the PCC OTC ‘Rules of Behavior’, ‘Privacy Statement’ and ‘Accessibility Statement’ available through links on the ELVIS sign-on screen, prior to using the system.
- Ensure that the necessary information security forms have been completed (‘PCC OTC Security Contact form’ which is used to designate the PCC OTC Security Contact(s), and the ‘PCC OTC User Access Request spreadsheet’ which is used to request user access to the ELVIS application). Only

authorized users can gain access to the ELVIS application. PCC OTC Security Contacts must submit a PCC OTC User Access Request spreadsheet for all access requests. Both forms can be found on the PCC OTC information website at <https://www.pccotc.gov/pccotc/Downloads/securityforms.htm>.

- Exiting users should no longer be in possession of POS equipment, i.e., access to or possession of the PCC OTC computer, USB flash drive, software or printed materials. Make certain that all POS equipment and printed material is available for the new person filling the position by ensuring that the equipment and material has been relinquished by the former employee.
- When an employee quits or changes their position, delete their access to both the POS and ELVIS. For information on how to delete users from the POS system, please refer to the *SAT* chapter of the *PCC OTC User Manual*, 'User Administration' section. For information on how to delete users from the ELVIS system, please refer to the *ELVIS* chapter of the *PCC OTC User Manual*, 'Accessing the *ELVIS URL*' section.
- Ensure that third-party service providers have adequate security in place with regard to the PCC OTC system.
- Establish procedures to follow when an employee fails to follow the security policies and procedures.

Physical and Environmental Protection

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection policy controls.

Agencies should control physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facility that are officially designated as publicly accessible) and verify individual access authorizations before granting access to the facility. The agency also controls access to areas officially designate as publicly accessible, as appropriate, in accordance with the agency's assessment of risk.

Effects on PCC OTC

- ❖ Agencies control physical access to all PCC OTC equipment including the screen display to prevent unauthorized individuals from observing/viewing the screen's display output.
- ❖ Agencies develop and keep current lists of personnel with authorized access to the area containing the PCC OTC system. Designated authorized individuals within the agency should review and approve access list at least annually. The agency promptly removes personnel no longer requiring access to the area containing the PCC OTC system.
- ❖ Agencies control physical access to the PCC OTC computer by authenticating visitors before authorizing access to the area that houses the PCC OTC system in areas that are not designated as publicly accessible.
- ❖ Agencies monitor physical access to the PCC OTC system to detect and respond to incidents.
- ❖ Agencies protect power equipment and power cabling for the PCC OTC system from damage and destruction.
- ❖ Agencies provide a short-term, uninterruptible power supply to facilitate an orderly shutdown of the PCC OTC system in the event of a primary power source loss. The hardware should be obtained through your internal procurement channels. A long term power supply option should also be considered in the event of an extended loss of the primary power source.
- ❖ Agencies control PCC OTC system-related items, i.e., hardware, firmware, software, when such items are entering and/or exiting the facility; and maintain appropriate records of those items.
- ❖ Individuals within the agency should employ appropriate PCC OTC security controls at alternate work sites. (*NIST Special Publication 800-46*).
- ❖ Agencies are responsible for securing PCC OTC scanners, peripheral equipment, checks, and other sensitive information in locked rooms, locked cabinets, or security containers supported by appropriate key control and other physical security controls.
- ❖ To the extent that the operational environment allows, PCC OTC scanners and check processing should be done in controlled environments such as steel cages, cashier cages, behind glass windows, and within offices where access to the PCC OTC system and peripheral equipment can be physically controlled.

In Summary

- Know who has physical access to the area that houses the PCC OTC computer.
- Ensure that unauthorized individuals cannot view the computer screen of the PCC OTC computer.
- Ensure that the PCC OTC hardware and software is secured, controlled, and monitored when entering or exiting the building.
- If, as in the case of military agencies, a ‘down-range’ environment is necessary, ensure that all security controls are in place to secure the equipment at the alternate work site.
- For military agencies and other agencies operating in remote or field locations, deploy appropriate physical security and access controls to limit unauthorized access to and unauthorized disclosure of PCC OTC processing areas and information.

Contingency Planning

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning policy controls.

The agency develops and implements a contingency plan for the PCC OTC system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the agency review and approve the contingency plan and distribute copies of the plan to key contingency personnel (*NIST Special Publication 800-34* provides guidance on contingency planning).

Effects on PCC OTC

- ❖ Agencies train personnel in their contingency roles and responsibilities with respect to the PCC OTC system and provide refresher training.
- ❖ Agencies test the contingency plan for the PCC OTC system at least on an annual basis to determine the plan's effectiveness and the agency's readiness to execute the plan. The test plan results are reviewed by the appropriate officials at the agency who initiate corrective action.
- ❖ Agencies review the contingency plan at least annually and revises the plan to address system/organization changes or problems encountered during plan implementation, execution, or testing.
- ❖ Agencies identify an alternate storage site and initiates necessary agreements to permit the secured storage of PCC OTC backup information which can include storage of backup hardware, i.e., extra scanners, and backup copies of software, etc.
- ❖ Agencies identify an alternate processing site and initiates necessary agreements to permit the resumption of the PCC OTC system operations for critical mission/business functions within a pre-determined time period, when primary processing capabilities are unavailable. The alternate site should be geographically separated from the primary processing site so as to not be susceptible to the same hazards.
- ❖ Agencies identify primary and alternate telecommunications services to support the PCC OTC system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions with a pre-determined timeframe when the primary telecommunications capabilities are unavailable.
- ❖ Agencies conduct backups of user-level and system-level PCC OTC information and stores backup information at an appropriately secured location. Each agency shall determine the appropriate frequency of these backups. Backup and restoration of this data should also be a part of the contingency plan testing.
- ❖ Agencies store backup copies of the operating system and other critical PCC OTC software in a separate facility or in a fire-rated container that is not collocated with the operational software.

- ❖ Agencies perform backups of the PCC OTC hard drive on a regular basis and store the backup in a secured location.
- ❖ Agencies employ mechanisms with supporting procedures to allow the PCC OTC system to be recovered and reconstituted to the system's original state after a disruption or failure.

In Summary

- Create a contingency plan and keep it current.
- Ensure people are trained to handle a contingency situation.
- Test the contingency plans yearly to ensure that hardware, communication medium, and software is in working order and current.
- Store a back copy of the POS software and printouts of user information in a secured area.
- Consider having a backup PCC OTC computer and PCC OTC related hardware, i.e., scanner, secondary storage, etc.
- Consider having PCC OTC related hardware and/or software backups also located off premises in a secured location. A backup of the PCC OTC hard drive should be performed on a regular basis.
- Extra scanners can be ordered and stored at an alternate site as backups in case of a failure or disruption. For addition information on ordering extra scanners, please contact the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 4, option 5, option.
- In the event of a failure or disruption, scanners can be delivered overnight to locations within the 48 contiguous states. Delivery will take longer for areas outside of this zone.
- Consider alternate processing sites.

Configuration Management

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated contingency planning policy controls.

The agency develops, documents, and maintains a current, baseline configuration of the PCC OTC system and an inventory of the system's constituent components.

Effects on PCC OTC

- ❖ Agencies should keep an inventory of the PCC OTC hardware and software. This inventory should include manufacturer, type, serial number, version number, and location (physical and logical within the architecture). This inventory should be kept current and changes should be documented.
- ❖ Ensure that PCC OTC security settings are defaulted to the most restrictive mode and should not be changed.
- ❖ Agencies should restrict access to the configuration information set within the POS to a select few authorized individuals.

In Summary

- Keep a current, documented listing of all of the PCC OTC hardware and software.
- Periodically check to make certain that the PCC OTC SAT (System Administration Tool) configuration settings are set to the recommended defaults as follows:

To view the SAT 'System Configuration' settings, an authorized user should sign on to the SAT and click the 'System' icon. Defaults for the General tab should be:

- Maximum failed Login attempt - 3
- Auto logout – should be checked and inactive minutes set to 15
- Batch Delete Age – 7 days (only 7 days of batches should be retained to reduce the amount of personal information stored on the hard drive of the POS computer and its secondary storage device. Higher amounts of stored P I I data equates to higher risk of accidental disclosure in the event of unauthorized access to the system, or malicious code.)
- Activity Log retention – 365 day

(See *SAT chapter of the PCC OTC User Manual* for complete instructions)

- Only the designated POC's (Point of Contact) or security contacts should be allowed access to the PCC OTC SAT.
- The POS activity log should be regularly reviewed for suspicious activity. Evidence or indicators of increased risks to the PCC OTC system and associated information must be responded to with more aggressive audit monitoring, more frequent review of audit logs, and the use of additional monitoring tools as appropriate. The activity log can be accessed by authorized personnel via the SAT and clicking on the 'Activity' icon. A complete explanation on how to read the activity log can be found in the *SAT chapter of the PCC OTC User Manual*, 'User Administration' section.

System Maintenance

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the system maintenance policy and associated system maintenance policy controls.

Effects on PCC OTC

- ❖ The system maintenance policy ensures that the agency schedules, performs, and documents routine preventative and regular maintenance on the PCC OTC components in accordance with the manufacturer or vendor specifications and/or agency requirements.
- ❖ All maintenance activities are controlled whether the equipment is serviced on site or removed to another location.
- ❖ Remove sensitive information from the PCC OTC system components (if feasible) when the components must be removed from the facility when repairs are necessary. This can be accomplished by backing up the PCC OTC hard drive to another medium such as CDs or an external hard drive then deleting the PCC OTC from the computer. When repairs have been complete, the data can then be restored. Secondary storage devices that contain sensitive data, i.e., flash drives, zip disks, CD-ROMs, and smart cards should be removed from the computer prior to servicing and stored in a secure location.
- ❖ Agencies approve, control, and monitor the use of maintenance tools used on the PCC OTC system, and maintains the tools on an ongoing basis.
- ❖ Agencies maintain a list of personnel authorized to perform maintenance on the PCC OTC system. Only those authorized personnel should be allowed access to perform maintenance on the system.

In Summary

- Regularly scheduled preventative maintenance should be performed on the POS computer, i.e., disk optimization tools, virus checking tools, etc., by authorized personnel only. Contact your local I T department for information on the tools authorized for use by your agency.
- If a component needs to be removed for repairs, all sensitive information should be removed. P I I may be contained in the form of names, account numbers, social security numbers, etc., within a POS batch on either the computer's hard drive or secondary storage. This also applies to repairs on LAN drives that may be used as a primary or secondary storage area for POS batch data.
- For agencies located in a dusty/sandy environment, PCC OTC computer equipment (computers and scanners) should be regularly cleaned with canned air.

System and Information Integrity

N I S T Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity policy controls.

Effects on PCC OTC

- ❖ Agencies identify information systems containing proprietary or open source software affected by recently announced software flaws and potential vulnerabilities resulting from those flaws. The agency should promptly install new released security relevant patches, service packs, and hot fixes, and test patches, service packs, and hot fixes for effectiveness and potential side effects on the PCC OTC before installation. (*N I S T Special Publication 800-40* provides guidance on security patch installation)
- ❖ Agencies implement malicious code protection on the PCC OTC system that includes a capability for automatic updates. Agency employs virus protection mechanisms at critical information system entry and exit points, i.e., firewalls, electronic mail servers, remote-access servers at workstations, servers, or mobile computing devices on the network and uses the virus protection mechanisms to detect and eradicate malicious code, i.e., viruses, worms, Trojan horses that can be transported by email, email attachments, internet access, removable media such as diskettes, CDs or flash drives, or by exploiting vulnerabilities.
- ❖ Virus protection mechanisms should be updated whenever new updates are available.
- ❖ Agencies employ tools and techniques to monitor events on the PCC OTC system, detect attacks, and provide identification of unauthorized use of the system. This applies to both the POS computer and any computer used to access the ELVIS system.
- ❖ Agencies implement tools to prevent spam and spyware.
- ❖ Agencies restrict information input to the PCC OTC system to authorized personnel only.
- ❖ Agencies check the PCC OTC information input for accuracy, completeness, and validity. PCC OTC information includes the scanned check data, and all input fields such as the dollar amount and user defined fields.
- ❖ The agencies identify and handle error conditions in an expeditious manner.
- ❖ The agencies handle and retain output, e.g., reports, check images, etc., from the PCC OTC in accordance with policy and operational requirements.

In Summary

- Protection against viruses, spyware and all other forms of malicious code on both the PCC OTC computer and all removable media used on the PCC OTC system (diskettes, CDs, flash drives) should be in place.
- Although the N I S T 800-53 document recommends keeping your computer up to date with the latest security patches, hot fixes and service packs, it is up to each agency to determine the feasibility of installing every patch or fix and installation may need to be considered on a case-by-case basis.

Consult your network support staff for more information. Only Windows 2000, Service Pack 4 and Windows XP Professional, Service Pack 2 have been validated to work after POS 5.4 is freshly installed. Other variations of Operating System Service Pack releases were upgraded and tested.

Please contact the

PCC OTC Customer Service staff for information about specific SP version validation.

- Regular updates to the virus protection software should be applied.
- Only authorized personnel should have access to the PCC OTC system. If using backup personnel to perform PCC OTC duties for both the POS and ELVIS, backups should be issued their own unique login ID and password. Logins and passwords should never be shared under any circumstances.
- Verification practices should be used to ensure accuracy of input. Batch control options can be setup by authorized personnel by logging into the POS and choosing, 'File', 'Configuration' and setting the batch control options on the 'Application Tab'. Batch Control is an optional feature that can be used as a batch balancing tool to ensure that the number of batched keyed and their respective dollar amounts have been accurately input. A complete explanation of how to use these settings for maximum control can be found in the *Daily Processing* chapter of the *PCC OTC User Manual* in the 'Batch Control' section.
- Verification practices can also include the use of the POS Batch List feature, to verify batch transmission totals. For a full explanation of how to use the Batch List feature, please refer to the *Daily Processing* chapter of the *PCC OTC User Manual* in the 'How to View and Print a Batch List' section. Using this practice can assist in the identification of errors and their effective handling, and lessen the possibility of fraudulent activity.
- To prevent duplicate processing of checks, checks may be hand stamped with 'Electronically Processed' after the transaction is complete and the check has been scanned. The EC6000i and EC7000i scanners can also be setup to automatically stamp the front of the check with the words, 'Electronically Presented', once the transaction is complete. For instructions on setting up the scanner to stamp the checks, please refer to the *Appendix* Chapter of the *PCC OTC User Manual*, 'Setting the EC6000i and EC7000i scanner to Frank Acknowledgments' section.

Media Protection

N I S T Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented media protection policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the media protection policy and associated system and information integrity policy controls.

Due to the nature of the transaction information which includes check images, the PCC OTC media that stores this information is considered PII and must be secured. The PCC OTC media to be protected includes both digital media, i.e., diskettes, external/removable hard drives, LAN drives used for PCC OTC data retention/storage, flash/thumb drives, compact disks, digital video disks, and non-digital media, i.e., paper, microfilm and checks not returned to the check writer. This control also applies to portable and mobile computing and communications devices with information storage capability, i.e., notebook computers, personal digital media assistants, and cellular telephones.

Effects on PCC OTC

- ❖ Agencies ensure that only authorized users have access to PCC OTC information in printed form or on digital media removed from the information system.
- ❖ Agencies affix external labels to removable PCC OTC storage media and PCC OTC system output indicating the distribution limitations and handling caveats of the information. Certain media may be exempted from this labeling as long as they remain within a secure environment.
- ❖ Agencies physically control and securely store the PCC OTC system media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media.
- ❖ Agencies sanitize PCC OTC system digital media using approved equipment techniques and procedures. Sanitization is the process used to remove information from digital media such that information recovery is not possible. (N I S T Special Publication 800-36 provides guidance on appropriate sanitization equipments, techniques, and procedures.)
- ❖ Agencies sanitize or destroy PCC OTC digital media before its disposal or release for reuse, to prevent unauthorized individuals from gaining access to and using information contained on the media. (N I S T Special Publication 800-36 provides guidance on appropriate sanitization equipments, techniques, and procedures.)
- ❖ Agencies physically control and securely store PCC OTC system media within a controlled area.

In Summary

- Only authorized users should have access to printed and digital media used for PCC OTC. This means all printouts, hard disks, LAN drives, external hard disks, diskettes, CDs, zip disks, smart cards, and USB flash drives.
- Store and label all removable media (both digital and paper) in a secured location. Labeling could include the restrictions on distributing the media and warnings on handling of the media.
- Properly remove all PCC OTC related data prior to destruction or reuse. Information stored on the PCC OTC's hard drive, secondary storage drive, and printed media may contain personally identifiable information (PII) in the form of names, account numbers, social security numbers, etc. within a POS batch.
- PCC OTC paper output such as batch lists, report printouts, and scanned checks not returned to customers contain P I I information and must be destroyed by shredding. This type of output should never be thrown away with other office trash without shredding.
- Consider additional encryption protection of the information that is contained on the secondary storage drive. The POS provides a minimum level of encryption to the data on the secondary storage drive but additional encryption protection may be used. If additional levels of encryption are used, agencies must ensure that the data can be decrypted in the event that the data needs to be restored using the POS 'Batch Recover' function. Decryption will typically involve the use of a password. If the additional level of encryption cannot be removed, the POS will be unable to read the batch data and the batch recovery function will fail.

Incident Response

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented incident response policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the incident response policy and associated system and incident response policy controls.

Effects on PCC OTC

- ❖ Agencies train personnel in their security incident response roles and responsibilities with respect to the PCC OTC system and provides refresher training.
- ❖ Agencies track and document PCC OTC system security incidents on an ongoing basis.

Agencies expeditiously report all PCC OTC system security incidents of theft, loss, or data/PII compromise (known or suspected) to the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 4, option 5, option 4, and their own internal authorized security personnel.

In Summary

PCC OTC Point-of-Contacts and users should monitor the PCC OTC system for possible security incidents and report any suspected incidents to the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 4, option 5, option 4 or via email at FMS.OTCChannel@citi.com.

Awareness and Training

N I S T Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training policy controls.

Security awareness and training ensures that all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to PCC OTC system and thereafter, at least yearly. Appropriate content of security awareness must be determined and based on the specific requirements of the PCC OTC system. The agency's security awareness program should be consistent with the requirements contained in 5 CFR Part 930.301 and with the guidance in N I S T Special Publication 800-50.

Effects on PCC OTC

- ❖ Users should be familiar with the POS and ELVIS password requirements as outlined in the *PCC OTC User Manual, Appendix R*.
- ❖ Users should be familiar with the ELVIS Security Guidelines which applies to both the POS and ELVIS as outlined in the *PCC OTC User Manual, ELVIS Chapter*.

In Summary

Information that is covered in the PCC OTC Security Awareness Training should include:

- Prevent others from watching while passwords are entered. Prevent others from guessing your password - do not use names of persons, places, or things that can be easily identified with you.
- Login IDs and passwords should never be shared.
- If your password has been compromised, it must be changed immediately.
- Unauthorized use of the system must be reported to Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 4, option 5, option 4 or via email at FMS.OTCChannel@citi.com.
- Log off of the system (both POS and ELVIS) whenever you leave your computer unattended by clicking on the 'Logout' button on the menu or clicking the 'X' at the upper right corner of the screen to prevent unauthorized access to the system.
- Security contacts or Point-of-Contacts should be kept current. As soon as an agency is aware of a change in personnel, a new person should be assigned the duties of the security contact to take the place of the exiting person. The exiting person's access should be deleted from both the POS and ELVIS.
- The POS comes with an 'admin' password. The PCC OTC security personnel, or POC's, should be trained on the proper handling of this user and it's associated password. Proper handling includes writing down the password and locking it up. Since the password will need to be changed every 90 calendar days it is important that the written password is updated whenever the password is changed. It should only be available to the POC. For complete information, please refer to *Appendix* chapter of the *PCC OTC User Manual*, section '*Appendix M, Personnel Change Over*'.

- Users should be familiar with the Rules of Behavior, Privacy Statement, and Accessibility Statement prior to using the system. The Rules of Behavior, Privacy Statement, and Accessibility Statement can be found as links at the bottom of the ELVIS sign-on screen.