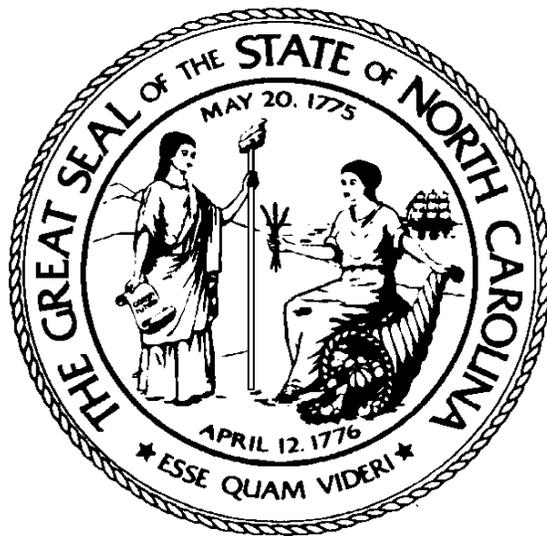


Security Administrator's Workshop

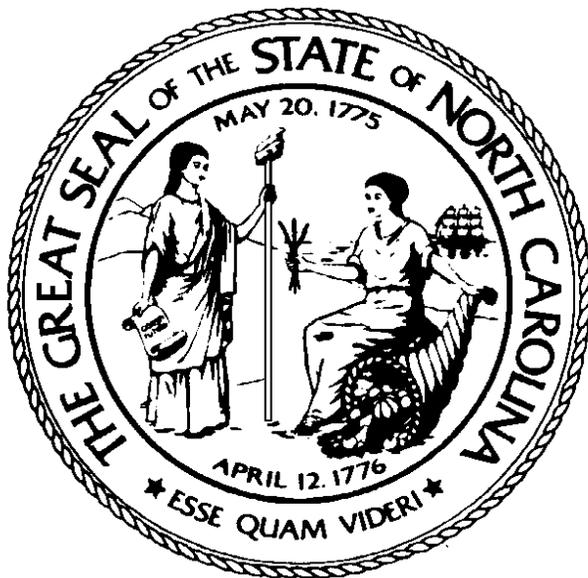


State of North Carolina

NC Accounting System

North Carolina Accounting System
Security Administrator's Workshop

Training Course
5th Edition



David T. McCoy
State Controller
September 1, 2008

This training was prepared by
The Office of the State Controller
<http://www.osc.nc.gov>

Contact Information

NCAS Support Services

(919) 707-0795

BEACON Training

(919) 707-0756

TABLE OF CONTENTS

Purpose of the Security System.....	1
Purpose of the Security System	1
Site Access Security.....	1
North Carolina Accounting System (NCAS) Security	1
OSC/Agency Security Responsibilities	3
Access Levels	5
Security Implementation Access Levels.....	5
CICS Resource Access Control Facility	5
Security Letters.....	6
Obtaining A CICS/RACF Operator ID.....	9
Deleting a CICS/RACF Operator ID	9
DCI Restrictive Security.....	9
Obtaining a DCI Operator ID	10
Deleting a DCI Operator ID	10
OSC Support Services Center Security Information	11
DCI Selective Security And Extended Product Security.....	11
Application Level Security	12
Obtaining DCI Selective Security	12
Deleting DCI Selective Security.....	13
Information Expert Security.....	15
Agency Libraries.....	15
Secured Public Libraries	15
Shared Public Libraries	16
NCAS Security Application Flowchart.....	17
NCAS Security Application Internal NCAS Password Security Flowchart	19
NCAS Security Application.....	21
NCAS Password Security for Setting Up NCAS Security.....	21
FORMS	23
(Your Agency) INTERNAL SECURITY REQUEST FORM	24
(Your Agency) Internal Security Request Form Descriptions	25
NCAS SECURITY REQUEST FORM	26
NCAS Security Request (OSC SEC01) Field Definitions	27
SELECT SYSTEMS TO BE ACCESSED.....	28
OSC SECURITY SIGN-OFF	29
APPLICATION PROFILE OR OPERATOR ID # APPLIED	29
NCAS Operator Restriction Form (OSC SEC02) Field Definitions.....	31
NCAS CHANGE OPERATOR SECURITY PROFILE FORM.....	34
NCAS Change Operator Security Profile Form (OSC SEC03) Field Definitions	35
CHANGE	35
SELECTIVE SECURITY RESTRICTIONS INCLUDE:.....	36
NCAS INFORMATION EXPERT SECURITY REQUEST FORM.....	38
NCAS Information Expert Security Request Form (OSC SEC04) Field Definitions	39

NCAS Security Reports	45
NCAS Agency Security Reports.....	46
NCAS Application Security Reports	46
DCI User File Reports.....	49
List of DCI Users Security Reports	49
DCI User Files.....	51
DCI User Table OSC Maintenance Reports	51
Using the NCAS Information Guide (SIG) to Access Security Profiles.....	53
QUICK REFERENCE GUIDE	55
NCAS Password Security	55

Purpose of the Security System

Purpose of the Security System

The role of security in a data-processing system is to protect an organization's resources from unauthorized access, modification, or destruction. An effective security program addresses both intentional and accidental breaches of security and emphasizes the development of complete controls and NCAS Password Security. These controls and NCAS Password Security include the automated security systems and the NCAS Password Security for backup, recovery, fraud protection, site access, and protection against acts of God.

Site Access Security

The Information Technology Services (ITS) division of the Department of Commerce is responsible for the physical protection of the computer site (e.g., the CPUs, tapes). The site security responsibilities include guards, closed circuit TV, security cards for access to certain sensitive areas, and pushbutton combination locks. ITS also provides secure storage vaults or safes, both on and off site, for protection of tapes and/or cartridges from theft or destruction from fire, flood, and other natural disasters. In the event of catastrophic failure of the ITS mainframe, ITS' responsibilities include restoring the operating system and system-related software and data files (e.g., TSO, CICS, RACF). The Office of the State Controller (OSC) is responsible for providing backup and recovery of all OSC application files including both software and data.

North Carolina Accounting System (NCAS) Security

The North Carolina Accounting System (NCAS) security prevents access by unauthorized operators, prohibits use and manipulation of restricted data by otherwise unauthorized operators, and protects the physical products of the system, such as checks, reports, printouts, and tapes. This security is accomplished through:

The OSC NCAS Security Administration Team, which oversees the system, has the final authority to extend or deny access to the NCAS. Agencies must enforce NCAS Password Security to control access to the NCAS CICS region by monitoring the Resource Access Control Facility (RACF) status of their personnel.

The OSC NCAS Security Administration Team is responsible for:

- **the defining of forms and NCAS Password Security** for identifying and tracking authorized operators.
- **the maintenance** of statewide security profiles for operator access based on job requirements.

OSC/Agency Security Responsibilities

SECURITY RESPONSIBILITIES	
OSC	AGENCY
NCAS CICS Region Access	
Extends or denies RACF group access to the NCAS CICS regions	Agency RACF Security Administrator assigns RACF IDs and enforces RACF security access
NCAS Security	
Oversees NCAS Security	Submits NCAS Security Letter
	Uses agency's internal controls, policies, and NCAS Password Security to prevent, detect, and correct abuse of NCAS security privileges
Restrictive/Selective Security	
Maintains the DCI Restrictive Security, DCI Selective Security, and Extended Product Security	Completes Authorized Agency Security Administrator(s) Letter
	Establishes and reviews the DCI Selective Security and Extended Product Security for each agency operator
NCAS Security Request Forms	
Processes NCAS Security Request forms	Applies for NCAS operator IDs via NCAS Security Request forms
Returns incomplete or inaccurate forms to the agency	Forwards properly completed and approved original Security Request forms to the OSC NCAS Security Administration Team
Keeps original security request forms	Retains agency copy
Does not allow alternative or agency designed forms	Attaches OSC SEC01 form to all initial operator security requests
Processes original forms and accepts telephone requests (with faxed copies) in emergency situations only	Notes the date of a faxed/telephone request on the original Security Request form and forwards original to OSC
NCAS Operator ID Number	
Assigns NCAS operator ID numbers and passwords	Notifies agency operators of their assigned NCAS operator ID numbers
	Ensures that operators change initial password at first sign on
IE Libraries	
Assigns I.E. libraries	Authorizes agency staff membership in operator groups
Maintains I.E. secured public libraries	Maintains agency libraries
DCI User Transaction Files	
Maintains operator profile data	Maintains Agency Sort data
	Requests that OSC set up a formatted transaction file
NCAS Security Reports	
Executes and spools security reports to X/PTR on a weekly basis	Reviews security reports in X/PTRX/PTR, verifies that each security request to OSC has been correctly completed, and notifies the OSC NCAS Security Administration Team of any discrepancies
Reset Passwords	
Resets NCAS passwords for Agency Security Administrators	Agency Security Administrator(s) requests that the OSC Support Services Center reset an operator's password
OSC NCAS Support Services Center	
Provides client support at (919) 875-HELP (4357)	Provides prompt and timely notification to OSC NCAS Security Administration Team of any problems, violations, or changes with an operator's access rights

Access Levels

Security Implementation Access Levels

The NCAS online systems provide multiple levels of automated security utilizing two separate security systems: the IBM Resource Access Control Facility (RACF) and the DBS Data Communication Interface (DCI). The OSC NCAS Security Administration Team defines any operator needing access to the NCAS and authorizes an operator's access to both security systems.

The NCAS Security System is implemented as a hierarchy. It does not permit access to the next security level without passing each previous security access level. The three security access levels are:

CICS RACF ID	This level controls access to the ITS mainframe and permits access to the NCAS CICS region where the online NCAS resides.
DCI RESTRICTIVE SECURITY	This level controls access to the NCAS application environment and permits access to a specific application system (e.g., General Ledger, Accounts Payable, Fixed Assets).
DCI SELECTIVE SECURITY AND EXTENDED PRODUCT SECURITY	This level controls access to screens and data within an application system. This application level security permits or denies an operator's access to specific screens within an application and to certain controls (e.g., buying entity, paying entity, company).

CICS Resource Access Control Facility

IBM's RACF is a security package used on mainframe computers. It consists of a database of security profiles that relate to users, groups, data sets, and general resources (e.g., terminals, disk packs, and CICS regions). Because RACF provides system-wide security, only certain individuals are authorized to define operators and resources. ITS/SCC (State Computer Center) maintains a tight control over these individuals.

RACF security is the first level of the NCAS security hierarchy and controls the initial entry to the NCAS. Agencies enforce the RACF security access. Some agencies have a designated RACF Technical Administrator. This person adds and/or creates a RACF operator ID for any new or existing agency personnel who need access to the NCAS. Each agency is responsible for its own policies and NCAS Password Security for the creation of RACF operator IDs.

NOTES

Once the agency RACF Technical Administrator has created the RACF operator ID for a prospective NCAS operator, he/she then attaches this operator ID to a NCAS RACF group. This RACF group definition permits access to the NCAS CICS regions. When the agency defines a NCAS RACF group, they must send a memo to the Information Expert (I.E.) NCAS Administrator at OSC. Only the OSC I.E. NCAS Administrator can permit a RACF group access to the NCAS CICS regions. The OSC I.E. NCAS Administrator maintains copies of all forms.

An agency that does not have its own RACF Technical Administrator should use the ITS/SDS (System Development Section) RACF Administrator. The ITS/SDS RACF Administrator follows the same NCAS Password Security as above for adding a new CICS/RACF operator with access to the NCAS.

Security Letters

Before an agency is permitted use of a NCAS/CICS region for NCAS business purposes, the agency must complete two security letters.

- NCAS Security Letter

The agency **must submit** the **NCAS Security Letter** before the OSC NCAS Security Administrator approves its use of a NCAS CICS region for business purposes. The agency's Chief Executive Officer and Chief Fiscal Officer **must sign** the NCAS Security Letter submitted on **agency letterhead**. The NCAS Security Letter must contain the information as specified in the sample letter (see the following example). Each agency should review this manual in order to be aware of its responsibilities prior to submitting the letter to the OSC and making initial application for entry to the NCAS.

The NCAS Security Letter must be addressed to:

*Office of the State Controller
Security Administrator/OSC Support Services Center*

- Authorized Agency Security Administrator(s) Letter

After completing the NCAS Security Letter, each agency receives the **Authorized Agency Security Administrator(s) Letter** from OSC (see the following example). The agency head should identify the authorized Agency Security Administrator(s), sign, and return the letter to OSC. The OSC NCAS Security Administration Team keeps the Authorized Agency Security Administrator(s) Letter on file and accepts security forms signed by the authorized individuals only.

The Authorized Agency Security Letter must be addressed to:

*Office of the State Controller
Security Administrator/OSC Support Services Center*

PREPARE ON YOUR AGENCY LETTERHEAD

NCAS Security Letter

Date

Mr. David McCoy
Office of the State Controller
1410 Mail Service Center
Raleigh, North Carolina 27699-1410

Dear Mr. McCoy:

Pursuant to the North Carolina Accounting System (NCAS) security requirements; we, [*Insert Agency Name*], confirm, to the best of our knowledge and belief, the following:

1. We have read and agree to comply with the Office of the State Controller (OSC) NCAS policies and procedures as stated in the North Carolina Accounting System, Systems Information Guide. http://www.ncosc.net/sigdocs/sig_docs/sigDocumentation.html
2. We are primarily responsible for the security of our NCAS data:
 - Accessing the NCAS CICS region, which grants an operator the initial entry point to the NCAS through the assignment of RACF IDs, is an agency-controlled function.
 - Once inside the NCAS, the agency specifies the operator's access to functions and processing capabilities.
3. We have controls, policies, and procedures designed to prevent, detect, and correct abuse of the NCAS security privileges within our agency. We understand that it is each agency's responsibility to review each profile and match the profile to each operator's job functions.
4. We agree to notify the OSC promptly of any problems, violations, or changes with an operator's access rights. Timely notification is essential when an operator changes job function and/or leaves the agency.
5. We realize that negligence in the area of security enforcement of operators with update rights exposes the agency to the risk of unauthorized access and tampering with agency data.
6. We understand that access to Information Expert Reporting (I.E.) activities does not grant an operator the ability to update or alter data. Reporting functions provide inquiry, display, and read-only capabilities.
7. We understand that when an agency is restructured and/or changes in personnel occur, it will be the agency's responsibility to update this letter and return it to the above address.

Agency Head/Director Signature

Chief Fiscal Officer Signature



State of North Carolina
Office of the State Controller

Michael F. Easley, Governor

David McCoy, State Controller

Current Date

TO: NCAS Chief Fiscal Officers
FROM: David McCoy, State Controller
SUBJECT: Agency Security Administrator Authorization

It is important that proper North Carolina Accounting System (NCAS) security authorizations and access requirements be established and continually maintained for an agency's staff. Agency restructuring and changes in personnel require updates to the agency security authorization information. Each agency is responsible for reviewing each profile and matching the profile to each operator's job functions. Agencies must use internal controls, policies and procedures to prevent, detect and correct abuse of NCAS security privileges. Each agency administrator agrees to the OSC disclaimer statement on personal identifying information (see the NCAS Security Policy for the statement).

Please list the individuals from your agency who are designated as Agency Security Administrators and have authority to sign the NCAS Security Request form, OSC SEC01. When the OSC SEC01 form is signed by one of the appointed individuals, and all accompanying security forms are accurately completed; the OSC NCAS Security Administrator will authorize NCAS system access to the operator identified on the security form(s). Return the completed security authorization information below to the OSC NCAS Security Administrator, OSC NCAS Support Services, Office of the State Controller.

Please contact the OSC NCAS Support Services section at 875-HELP (4357) if you have any questions regarding security procedures.

_____ Name	_____ Email Address	_____ Telephone
_____ Title	_____ Security Administrator Signature	_____ Date
_____ Name	_____ Email Address	_____ Telephone
_____ Title	_____ Security Administrator Signature	_____ Date
_____ Name	_____ Email Address	_____ Telephone
_____ Title	_____ Security Administrator Signature	_____ Date
_____ Name	_____ Email Address	_____ Telephone
_____ Title	_____ Security Administrator Signature	_____ Date
Signature: _____	_____ Chief Fiscal Officer	_____ Date
_____ Agency Name		

MAILING ADDRESS
1410 Mail Service Center
Raleigh, NC 27609-1410

Telephone: (919) 981-5454
Fax Number: (919) 981-5567
State Courier: 56-50-10
Website: www.ncosc.net

LOCATION
3512 Bush Street
Raleigh, NC

An Equal Opportunity/Affirmative Action/Americans With Disabilities Employer

Obtaining A CICS/RACF Operator ID

NOTES

An operator who needs a CICS/RACF operator ID with access to the NCAS should contact his/her supervisor. Agency supervisory personnel can direct their staff members concerning agency NCAS Password Security for obtaining a CICS/RACF operator ID for NCAS access.

Deleting a CICS/RACF Operator ID

It is the agency's primary responsibility to monitor operators and remove operators as soon as they are no longer authorized to process in the NCAS. These operators are **immediately** removed from the agency NCAS RACF group.

In most cases, an employee cannot access the NCAS if he/she has left state government and has had his/her RACF ID removed. However, in the special case of an employee who transfers from one state agency to another, removing the RACF ID is not sufficient to safeguard agency data files. The operator is still able to access the data of the prior agency after obtaining a RACF ID from the new agency, unless the agency has notified the OSC to remove application security access.

DCI Restrictive Security

DCI Restrictive Security controls operator authorization, operator passwords, and access to NCAS online applications. The NCAS uses the operator, password, and application portions of restrictive security. The OSC NCAS Security Administration Team maintains the DCI Restrictive Security. Unless operators are specifically authorized, all access to the NCAS screens, functions, and data records is denied. The OSC NCAS Security Administration Team does not restrict NCAS operators to accessing applications from specific predetermined terminals.

Restrictive security is checked at two points: DCI sign on and DCI Main Menu selections. First, when any operator types the NCAS CICS transaction ID (MSAS or MSAR), DCI presents the NCAS SIGN ON screen. After the operator enters his/her assigned operator ID and password, DCI validates that the operator is defined to the NCAS and that the password is correct for that operator ID. If the operator ID and password are valid, DCI presents the NCAS main menu. The operator can only use one workstation at a time. If the operator attempts to sign on at another workstation before logging off the first, an error message occurs (i. e., OPERATOR XXXXXX ALREADY SIGNED ON).

The DCI Main Menu permits the operator access to application source systems (e.g., General Ledger, Accounts Payable, and Fixed Assets). This is the second point at which DCI Restrictive Security is evoked. The security program checks to see if the operator is authorized to access the chosen application. Restrictive security permits or denies access to the requested application any time an operator tries to move from one application to another.

NOTES

Obtaining a DCI Operator ID

The primary OSC security form is OSC SEC01. Security Request forms are located in the System Information Guide (SIG) and can be requested from the OSC Support Services Center. The Agency Security Administrator should complete and sign this form. Incomplete or inaccurate forms are returned to the Agency Security Administrator.

When adding new operators to the NCAS, the OSC NCAS Security Administration Team places primary importance on accuracy and verification of operator qualifications. The OSC NCAS Security Administration Team processes the OSC security forms as expeditiously as possible. The OSC has determined that restrictive security is defined in batch and updated in overnight processing. Each week OSC executes and spools security reports to the Systemware (X/PTR).

When signing on the first time, the operator must change the initial password. The Agency Security Administrator must ensure that initial passwords are changed at the first sign on. If the operator uses the initial password for an extended period of time, then he/she is subject to automatic revocation of access privileges. **Operators should keep security information confidential.** Audit trails, composed primarily of the operator ID, trace the activity within the NCAS. **System operators will be held responsible for any destruction or unauthorized activity caused by their operator ID.**

-  If the agency security NCAS Password Security require that an operator, who transfers from one agency location to another, is assigned a new NCAS operator ID, the Agency Security Administrator should **complete an ADD new operator ID request and a DELETE old operator ID request.** The Agency Security Administrator should attach the two requests and forward them to the OSC NCAS Security Administration Team.

Deleting a DCI Operator ID

The agency should complete a **NCAS Security Request Form, OSC SEC01** when an operator needs to be removed from the NCAS. The Agency Security Administrator should send the form to the OSC Security Administration Team at the OSC Support Services Center.

When the situation demands immediate removal of an operator from the system (e.g., agency transfers), verbal contact with the OSC Support Services Center can precede the OSC SEC01 form. To remove application level security, the Agency Security Administrator must notify the OSC NCAS Security Administration Team of the urgent nature of the request. The OSC NCAS Security Administration Team immediately removes operator access from agency-specific data and the NCAS screens.

OSC Support Services Center Security Information

NOTES

In the past, the OSC Support Services Center received large numbers of security processing requests on Thursdays. Security request forms received after Tuesday by the OSC Support Services Center may not be completed in time for the weekly Thursday night batch processing. If requests are received by Tuesday, the Support Services Center and Technical Applications staff can complete the necessary requirements prior to the Thursday night deadline for batch processing. However, large numbers of requests may require additional time.

The OSC Support Services Center no longer accepts faxed copies of the Security Request Form. If an emergency exists, the agency should first call the OSC Support Services Center to request approval to send a faxed copy of the form, sending the original form immediately thereafter using the standard means of delivery. No form should be faxed without first receiving approval from the OSC Support Services Center.

DCI Selective Security And Extended Product Security

DCI Selective and Extended Product Security are application specific security mechanisms. Application security controls the screens and the data that an operator can access. Once an operator has accessed a screen, application security controls the levels of data available. Within an agency, data that an operator is able to access is hierarchically defined by Financial Controller/General Ledger Companies, Accounts, and Centers, Paying Entities and/or Buying Entities, Catalog Entities, Warehouses, Accounts Receivable Companies and Credit Analyst Controls, and Fixed Assets Companies. This is a critical security area where the daily business operations of an agency take place. The NCAS database is created and maintained within the business functions of a specific NCAS application system. A combination of the agency's business functional needs and the costs of the associated security determine the appropriate level of security.

Application level security is defined for:

- Accounts Payable (**AP**)
- Accounts Receivable (**AR**)
- Budgetary Control (**BC**)
- Fixed Assets (**FA**)
- Financial Controller (**FC**)
- General Ledger (**GL**)
- Inventory (**IN**)
- Procurement Card (**PC**)
- Purchasing (**PS**)

NOTES

- Project Tracking (**PT**) (if applicable)

Information Expert has its own internal function and data security system. The I.E. system permits operators to report on their data; no business operational functions are performed. I.E. security is discussed in the *Information Expert Security* section.

Application Level Security

The OSC controls the application level security (refer to the *Forms* section) using information supplied by the agencies on:

- **OSC SEC01, NCAS Security Request Form**
- **OSC SEC02, NCAS Operator Restriction Form**
- **OSC SEC03, NCAS Change Operator Security Profile Form**

The OSC NCAS Security Administration Team maintains most applications online. Application security for the Fixed Assets systems is maintained offline in batch mode.

Operators may access only those controls (Financial Controller/General Ledger Companies, Buying Entities, Paying Entities, Catalog Entities, Warehouses, Accounts Receivable Companies, Credit Analysts, and Fixed Assets Companies) that are identified to their agency. An agency's business practices may dictate that an operator's access be further restricted to portions of the agency's data. By using form OSC SEC02, the Agency Security Administrator can restrict an operator to certain companies, accounts, and centers or ranges of accounts and centers. The system provides 45 lines that can be used for listing these restrictions. Restricting an operator to certain accounts limits all screens, including inquiry screens, to only the accounts and centers specified. It is the agency's responsibility to establish and review this level of security.

Screens are related to the business functions performed by the application (e.g., invoice entry, fixed asset maintenance, vendor maintenance, and cash application). For this reason, operator security profiles have been developed that relate screens to an operator's business functions and job assignments. These profiles include all processing screens necessary for an operator to perform his/her duties, plus any inquiry screens related to those duties. For example, the standard security profile developed for an Accounts Payable Processor includes invoice maintenance and any related Purchasing, Accounts Payable, Financial Controller, and General Ledger inquiry screens. It may be necessary to modify statewide operator security profiles to include agency-specific operational functions.

Obtaining DCI Selective Security

The primary OSC security form is OSC SEC01. Security Request forms are located in the SIG and can be requested from the OSC Support Services Center. The Agency Security Administrator should complete and sign this form. Incomplete or inaccurate forms are returned to the Agency Security Administrator.

If tighter selective security is desired beyond the agency level or an operator's functions change, the appropriate restrictions and/or changes must be indicated on forms OSC SEC02, NCAS Operator Restriction Form; OSC SEC03, NCAS Change Operator Security Profile Form; and/or OSC SEC04, NCAS Information Expert Security Request Form.

NOTES

The OSC NCAS Security Administration Team processes the security forms as soon as possible. As a part of the production process, the OSC executes and spools the security reports to X/PTR once a week. The Agency Security Administrator should view the security reports (e.g., OSCOP* Security Table Update OSC), verify that each security request has been correctly completed, and notify the OSC NCAS Security Administration Team of any discrepancies. It is the agency's responsibility to ensure that new operators have the correct security privileges and that they change their initial password the first time they sign on to the system.

-  An asterisk (*) in the job/group name represents a region-specific variable. Use **C** to reference report groups in the SCCP region. Use **F** to reference report groups in the NC23 region.

Deleting DCI Selective Security

The NCAS Password Security for deleting DCI selective security are the same as those for deleting a DCI operator ID. Refer to the *Deleting a DCI Operator ID* section.

Information Expert Security

Information Expert Reporting (I.E.) is a reporting tool that permits operators to design and run their own reports. Unlike the other applications, I.E. does not allow operators with I.E. access to enter or change any existing data. For this reason, I.E. application security access privileges are structured differently from the other systems such as Accounts Payable and Accounts Receivable, which perform business functions.

When I.E. is checked on form OSC SEC01, the NCAS Security Request Form, authorized operators may report on all data. Access to I.E. activities does **not** allow an operator to update or alter data. Reporting functions provide inquiry, display, and read-only capabilities. To finish the request, the Agency Security Administrator must complete the **OSC SEC04, Information Expert Security Request Form** (refer to the *Forms* section).

Agency Libraries

Reporting information is stored in I.E. libraries. The OSC NCAS I.E. Security Administrator does not assign individual libraries for each I.E. operator, but he/she provides each state agency a group of secured public libraries. Therefore, the agency operators share agency-secured public libraries. Only certain operators or groups of operators within that agency have access to update and view an agency-secured public library.

The Agency I.E. Security Administrator maintains the contents of the agency libraries and authorizes certain agency staff membership in the operator groups. The Agency I.E. Security Administrator should have access to TSO (Time-Sharing Option) and a good knowledge of JCL (Job Control Language).

The agency operators may copy RUN-STATEMENTS from the Public Libraries into their default libraries before submitting any reports. Because these are shared libraries, it should never be assumed that any member is as an operator last left it. The operator should always check the RUN-STATEMENTS before submitting a job. To ensure that the correct files are being read and that the reports are printed on the correct printer, the RUN-JCL and PRINT-JCL should also be checked.

Secured Public Libraries

Secured public libraries are shared by all state agencies. The OSC technical staff maintains them. The agency operator may copy from these libraries, but they cannot change any members. There is a public library for each application. The reports for the application are in the respective library.

NOTES

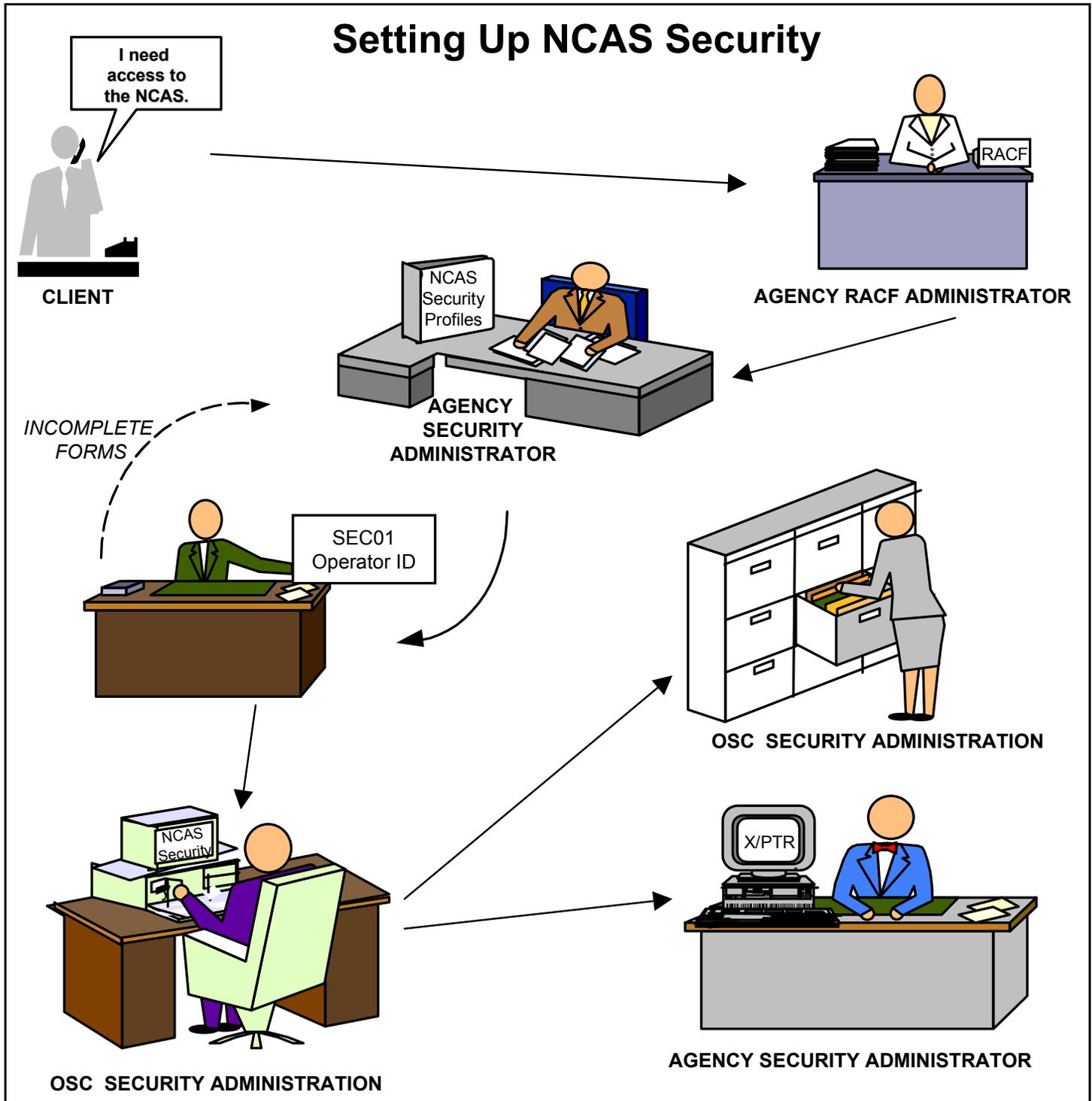
These secured public libraries include:

APPUBLIC	FCPUBLIC
ARPUBLIC	GLPUBLIC
BCPUBLIC	IEPUBLIC
CCPUBLIC	INPUBLIC
FAPUBLIC	PSPUBLIC

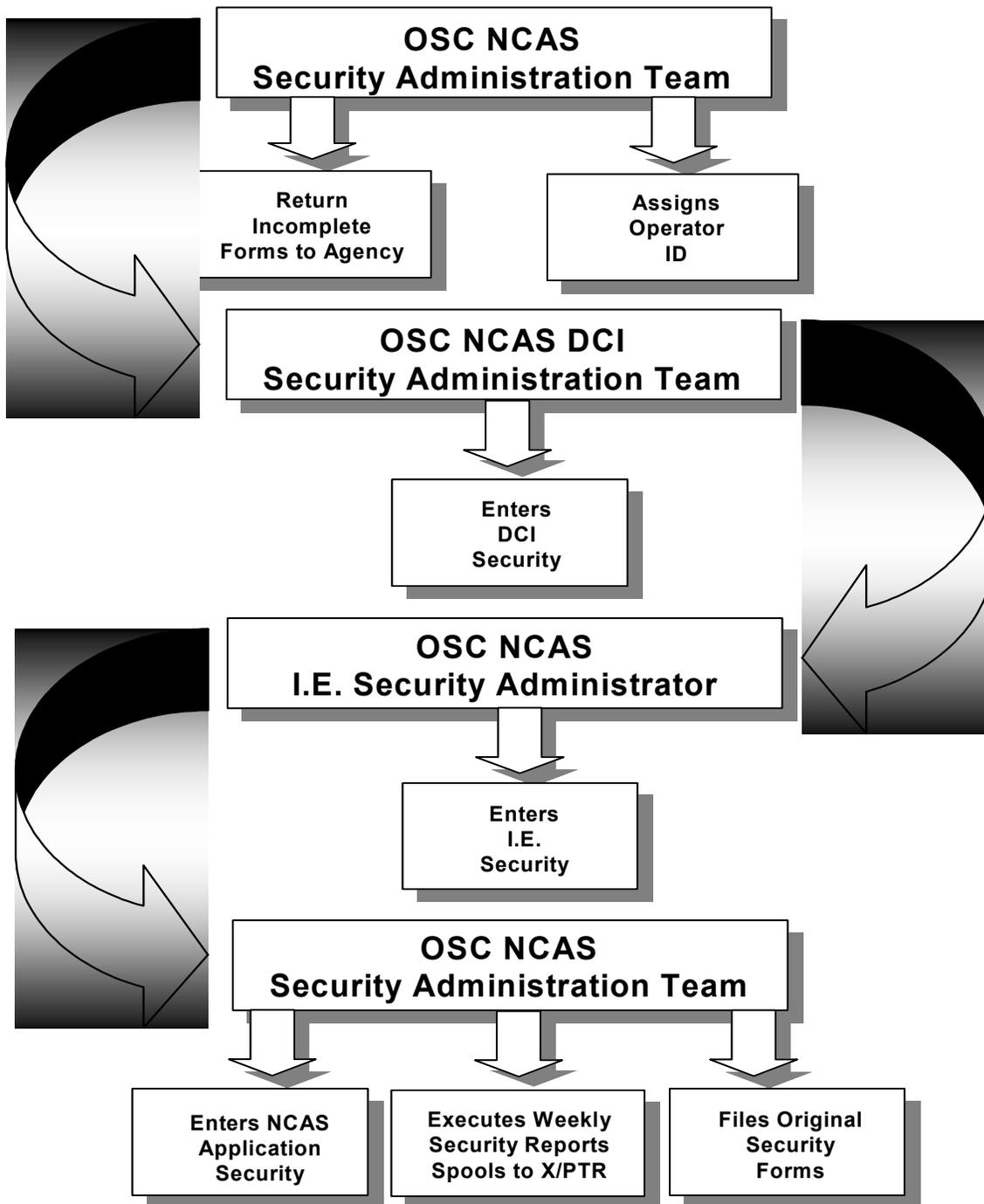
Shared Public Libraries

NCPUB is a library that is shared by all agencies for copying and changing members. NCPUB was established as a library in which reports can be shared and passed among agencies. For example, an operator at DPI can copy a sample report into NCPUB for an operator at DOC. The DOC operator can then copy the report into a DOC agency library. Development or reporting should not occur in this library.

NCAS Security Application Flowchart



NCAS Security Application Internal NCAS Password Security Flowchart



NCAS Security Application

NCAS Password Security for Setting Up NCAS Security

1. All persons who need access to the NCAS software must first obtain RACF security from their agency's RACF Security Administrator. Appropriate agency NCAS Password Security should be followed.
2. The Agency Security Administrator must complete a **NCAS Security Request Form, OSC SEC01**, for each operator who needs to be added, deleted, or who needs security access privileges changed in the NCAS. Additional security restrictions must be indicated on the **NCAS Operator Restriction Form, OSC SEC02**. Security restrictions to an operator's profile for any NCAS application are indicated on the **NCAS Change Operator Profile Form, OSC SEC03**. Operation restrictions and additions in Information Expert are defined on the **Information Expert Security Request Form, OSC SEC04**.
3. The authorized Agency Security Administrator reviews the form(s) for completeness and accuracy. Using the security for OSC SEC01 and any additional security restrictions on forms OSC SEC2, OSC SEC03, and OSC SEC04, he/she defines the appropriate profiles for each application requested. The Agency Security Administrator forwards the original agency approved security request to the OSC Security Administrator, Support Services Center, and retains a copy for the agency files.
4. For approved applications, the OSC NCAS Security Administrator signs and dates the **OSC Security Authorization** on form OSC SEC01. He/she assigns and writes the operator ID in the appropriate space. The Agency Security Administrator returns any incomplete or inaccurate security requests.
5. The security forms are forwarded to the OSC NCAS Security Administration Team. After completing DCI Restrictive Security, he/she signs and dates the OSC SEC01 form. If I.E. has been requested, the Security Administrator forwards the original application to the OSC NCAS I.E. Security Administrator, who sets up I.E. security. The I.E. Security Administrator signs and dates the OSC SEC04 form and forwards the original security form to the OSC NCAS Security Administration Team.

NOTES

6. The OSC NCAS Security Administration Team enters the operator's application security using the standard statewide or agency security profiles specified on form OSC SEC01 and/or additional restrictive security specified on forms OSC SEC02 and OSC SEC03. The OSC NCAS Security Administration Team completes the application security, signs, and dates the form(s). The security profiles are verified and any special remarks or notations are listed on the form.

7. Each week, the OSC executes and spools the security reports to X/PTR. The Agency Security Administrator should view the security reports, verify that each security request has been correctly completed, and notify the OSC NCAS Security Administration Team of any discrepancies. It is the agency's responsibility to ensure that a new operator changes his/her initial password the first time he/she signs on to the system. The original security request form(s) remains on file with the OSC NCAS Security Administration Team at the OSC Support Services Center.
 -  The OSC NCAS Security Administration Team does **not** accept original security set-ups or requests for security access from unauthorized agency personnel over the telephone. All security requests must pass through agency internal screening NCAS Password Security. A prospective operator or his/her supervisor must contact the Agency Security Administrator for assistance in applying for NCAS access.

FORMS

(Your Agency) INTERNAL SECURITY REQUEST FORM

<input type="checkbox"/> ADD	<input type="checkbox"/> CHANGE	<input type="checkbox"/> DELETE
------------------------------	---------------------------------	---------------------------------

Department/Division: _____

Operator Name: _____

Operator ID # (for changes & deletions): _____

RACF ID: _____ RACF Group: _____

Job Title: _____

NCAS Duties: (check all that apply)

<input type="checkbox"/> Enter Requisitions	<input type="checkbox"/> Accounts Receivable
<input type="checkbox"/> Enter Purchase Orders	<input type="checkbox"/> Inventory Processing
<input type="checkbox"/> Enter Invoices	<input type="checkbox"/> Budget Officer
<input type="checkbox"/> Enter Vendors	<input type="checkbox"/> SBM
<input type="checkbox"/> Enter Budget Entries	<input type="checkbox"/> Other (explain) _____
<input type="checkbox"/> With End Approval _____	
<input type="checkbox"/> Without End Approval _____	

Inquiry Inquiry

Note any specific ranges required: (If you need additional space, please attach a separate page.)

Company Access	Account Access	Center Access
	From To	From To

Requested By: _____ Date: _____

Approved By: _____ Date: _____

(Your Agency) Internal Security Request Form Descriptions

The (Your Agency) Internal Security Request Form is a suggested form to be used for agency internal use. This form should be modified to conform to agency requirements. It provides general information about the operator and the type of access that he/she will need in the system. After receiving this completed form, the Agency Security Administrator must then complete the appropriate OSC NCAS Security Request Forms.

ADD	Add a new operator to the NCAS
CHANGE	Change an existing operator's security to the NCAS
DELETE	Delete an existing operator from the NCAS
DEPARTMENT/DIVISION	The agency's department/division
OPERATOR NAME	Operator's <i>complete</i> name
OPERATOR ID #	Operator ID number assigned by OSC NCAS Security Administration Team
RACF ID	Mainframe system access defined to Resource Access Control Facility (RACF) assigned to the operator by the Agency Security Administrator
RACF GROUP	The RACF ID defined to a RACF Group by the Agency Security Administrator
JOB TITLE	The operator's job title
NCAS DUTIES	Check all that apply. For example, an Accounts Payable Processor may also check <i>Enter Invoices</i> and <i>Enter Vendors</i>
NOTE ANY SPECIFIC RANGES REQUIRED	Enter the specific company/account/center combinations that this operator needs to perform his/her duties
REQUESTED BY	Signature and date of the person that is requesting this security
APPROVED BY	Signature and date of the person that approves the requested security

NCAS Security Request (OSC SEC01) Field Definitions

The **NCAS Security Request Form, OSC SEC01**, is divided into two main sections. The first section is completed by the agency when requesting security access for an operator. The second gray section is for OSC use only.

AGENCY REQUEST

The **Agency Request** section is divided into two main areas. The first area provides general information about the requesting agency, the operator, and the type of request. The second area indicates the selected systems for operator use, the type of screen access, the profile definition, and signature authority.

AGENCY #	A two-digit OSC-assigned agency identifier. For example, the agency number for DOC is 42.
DIV NAME	If any agency has divisional locations, this field may identify the agency's division location for the operator. For example, a DOC operator may be located at the Division of Prisons (DOP).
REGION	P or NC23. Always required.
TYPE OF REQUEST	Indicate the type of security request: A = Add a new operator to the NCAS C = Change an existing operator's security D = Delete an existing operator from the NCAS N = Change name and password only. The following information is conditional , based on the type of request made: If A, include 2 and 3. If C, include 1, 2, and 3. If D, include 1 and 2.
¹ OPERATOR ID #	Operator ID number assigned by the OSC NCAS Security Administration Team, required if the type of request is a CHANGE or DELETE .
² OPERATOR NAME	Operator's <i>complete</i> name. Always required.
³ FOR SECURITY RESTRICTIONS, ATTACH FORMS OSC SEC02, OSC SEC03, AND/OR OSC SEC04	If the operator's security differs from the selected NCAS or agency security profiles, if additional selective restrictions are needed, or if I.E. security is requested, security forms OSC SEC02, OSC SEC03, and/or OSC SEC04 should be attached. It is conditionally required if the type of request is an ADD or CHANGE .
³ RACF ID	Mainframe system access defined to RACF is assigned to the operator by the agency's RACF Security Administrator. It is required if the type of request is an ADD operator, conditionally required if the type of request is a CHANGE .

³ RACF GROUP	The RACF ID is defined to a RACF Group by the Agency Security Administrator. It is required if the type of request is an ADD .
³ OPERATOR'S PHONE NUMBER	The operator's direct phone number is required if the type of request is an ADD . It is conditionally required if the type of request is a CHANGE .
³ OPERATOR'S FAX NUMBER	The operator's fax number is required if the type of request is an ADD . It is conditionally required if the type of request is a CHANGE .
³ OPERATOR'S EMAIL ADDRESS	The operator's email address is required if the type of request is an ADD or a CHANGE .

SELECT SYSTEMS TO BE ACCESSED

APPLICATION #	The application number is a two-digit number that identifies the application within DCI security.																				
APPLICATION ID	The application ID is a two-character identifier that represents the application system to be accessed. This is user information only.																				
	<table border="0"> <tr><td>AP</td><td>Accounts Payable</td></tr> <tr><td>AR</td><td>Accounts Receivable</td></tr> <tr><td>BC</td><td>Budgetary Control</td></tr> <tr><td>FA</td><td>Fixed Assets</td></tr> <tr><td>FC</td><td>Financial Controller</td></tr> <tr><td>GL</td><td>General Ledger</td></tr> <tr><td>I.E.</td><td>Information Expert</td></tr> <tr><td>IN</td><td>Inventory</td></tr> <tr><td>PS</td><td>Purchasing</td></tr> <tr><td>PC</td><td>Procurement Card</td></tr> </table>	AP	Accounts Payable	AR	Accounts Receivable	BC	Budgetary Control	FA	Fixed Assets	FC	Financial Controller	GL	General Ledger	I.E.	Information Expert	IN	Inventory	PS	Purchasing	PC	Procurement Card
AP	Accounts Payable																				
AR	Accounts Receivable																				
BC	Budgetary Control																				
FA	Fixed Assets																				
FC	Financial Controller																				
GL	General Ledger																				
I.E.	Information Expert																				
IN	Inventory																				
PS	Purchasing																				
PC	Procurement Card																				
INQUIRY ONLY SCREENS	To request inquiry screens, check the box by the appropriate application(s). A check in the Inquiry Screens box allows an operator to view data on inquiry menu selections.																				
	<table border="0"> <tr> <td style="vertical-align: top;">Warehouses</td> <td>List the warehouse controls for the requested screen access. Unless noted, the complete agency range is assumed for all screens. The exception is Usage Order processing screens.</td> </tr> <tr> <td style="vertical-align: top;">FA Levels</td> <td>The Fixed Asset Level 1/Level 2 must be listed for the requested screen access.</td> </tr> <tr> <td style="vertical-align: top;">BC Document END APPROVAL</td> <td>Operator ID(s) listed in the BC document END APPROVAL field(s) have the authority to end BC documents for the Operator ID listed at the top of the form. If an Operator ID is not specified, it is assumed that this operator can approve his/her own BC documents.</td> </tr> <tr> <td style="vertical-align: top;">I.E. ACCESS (YES)</td> <td>To request I.E. system access, check the box. Complete the OSC SEC04 form, NCAS Information Expert Security Request.</td> </tr> </table>	Warehouses	List the warehouse controls for the requested screen access. Unless noted, the complete agency range is assumed for all screens. The exception is Usage Order processing screens.	FA Levels	The Fixed Asset Level 1/Level 2 must be listed for the requested screen access.	BC Document END APPROVAL	Operator ID(s) listed in the BC document END APPROVAL field(s) have the authority to end BC documents for the Operator ID listed at the top of the form. If an Operator ID is not specified, it is assumed that this operator can approve his/her own BC documents.	I.E. ACCESS (YES)	To request I.E. system access, check the box. Complete the OSC SEC04 form, NCAS Information Expert Security Request.												
Warehouses	List the warehouse controls for the requested screen access. Unless noted, the complete agency range is assumed for all screens. The exception is Usage Order processing screens.																				
FA Levels	The Fixed Asset Level 1/Level 2 must be listed for the requested screen access.																				
BC Document END APPROVAL	Operator ID(s) listed in the BC document END APPROVAL field(s) have the authority to end BC documents for the Operator ID listed at the top of the form. If an Operator ID is not specified, it is assumed that this operator can approve his/her own BC documents.																				
I.E. ACCESS (YES)	To request I.E. system access, check the box. Complete the OSC SEC04 form, NCAS Information Expert Security Request.																				

COPY: NCAS OR
AGENCY SECURITY PRO-
FILE # OR A CURRENT ID#

To access the selected system screens, indicate a NCAS or Agency Security Profile number that should be copied.

REQUESTED BY

The signature (and date) of the Agency Security Administrator

OSC USE ONLY

The **OSC Use Only** section is divided into three main areas that define NCAS security assignment to the operator, security sign-offs, and OSC application verification.

OPERATOR ID #

NCAS Operator ID number assigned by the OSC
NCAS Security Administration Team member

OSC SECURITY SIGN-OFF

DCI SECURITY
COMPLETED BY

The signature (and date) of the OSC NCAS DCI Security Administrator. This signature indicates that the OSC NCAS DCI Security Administrator has approved and completed the DCI security.

I.E. SECURITY
COMPLETED BY

The signature (and date) of the OSC NCAS I.E. Security Administrator. This signature indicates that the OSC NCAS I.E. Security Administrator has approved and completed the I.E. security.

APPLICATION PROFILE OR OPERATOR ID # APPLIED
(VERIFICATION)

Any changes that the OSC Security Administration Team makes to the form will be noted on the appropriate lines. The OSC initials and dates all changes.

APPLICATION SECURITY
COMPLETED BY

When the application security is completed, the OSC NCAS Security Administration Team member stamps the form with the date of completion and position number of the employee processing the security request.

NCAS Operator Restriction Form (OSC SEC02) Field Definitions

The **NCAS Operator Restriction Form, OSC SEC02**, is used to indicate additional selective security restrictions. The form is divided into two main sections. The first section is general information to be completed by the agency. The operator's processing and inquiry capabilities are limited by the company/account/center combinations defined to Financial Controller (FC). The second gray section is for OSC use only.

OPERATOR NAME	Operator's <i>complete</i> name. Always required.
OPERATOR ID #	Operator ID number assigned by the OSC NCAS Security Administration Team member. This box should be blank when adding an operator. When changing an operator's access rights, this box should be completed. A separate OSC SEC02 form should be completed for each type of restriction.
AGENCY	Agency name or abbreviation (Department of Correction or DOC)
AGENCY #	A two-digit OSC assigned agency identifier. (For example, the agency number for DOC is 42.)
PROFILE #	Selected application number for that operator that corresponds to the profile listed on the SEC01 form
REGION	P or NC23. Always required.
DATE	Date of request
ADD	Check the ADD box if the indicated company/account/center range(s) is an addition to an operator's existing security restrictions or is the restricted security range for a new operator.
DELETE	Check the DELETE box if the indicated company/account/center range(s) is to be deleted from an operator's existing security restrictions. A separate OSC SEC02 form should be completed for each application.
FC	Financial Controller company/account/center ranges. FC limits security to all applications except GL.
GL	General Ledger company/account/center Because an operator is limited to 45 combinations, the Agency Security Administrator should identify ranges whenever possible.
PC	Agency, location, card number
ACCESS Y/N	Mark Yes (Y) to allow operator access. Mark No (N) to deny operator access.
COMPANY FROM/TO	GL company number

ACCOUNT FROM/TO	GL account number
CENTER FROM/TO	GL center number
ACCESS Y/N	Mark Yes (Y) to allow operator access. Mark No (N) to deny operator access.
AGENCY FROM/TO	The agency identifier (first two positions of company). Used to secure an individual to a particular agency.
LOCATION FROM/TO	The procurement card location assigned to the agency. Used to secure an individual to a particular location.
CARD NUMBER FROM/TO	The last 4 digits of the procurement card number. Used to secure a cardholder to a particular number.
REQUESTED BY	The signature (and date) of the Agency Security Administrator. This signature is required when the OSC SEC01 form is not attached.

**THIS PAGE INTENTIONALLY LEFT
BLANK TO FACILITATE
REPORT VIEWING**

NCAS CHANGE OPERATOR SECURITY PROFILE FORM

OSC FORM SEC03

OPERATOR NAME: _____	OPERATOR ID #:	<input style="width: 95%;" type="text"/>
AGENCY: _____	AGENCY #: _____	REGION: _____
CHANGE:	APPLICATION: <input style="width: 40px;" type="text"/>	NCAS OR AGENCY PROFILE NUMBER: _____

IF THE OPERATOR'S SECURITY DIFFERS FROM THE SELECTED NCAS OR AGENCY SECURITY PROFILE, INDICATE EACH SCREEN CHANGE. THE SELECTIVE SECURITY RESTRICTIONS LISTED BELOW SHOULD APPLY FOR **EACH** SCREEN ID INDICATED. NOTE SPECIFIC RESTRICTIONS TO COMPANY/ACCOUNT/CENTER ON FORM OSC SEC02.

THE FOLLOWING SCREEN(S) DIFFER FROM THE PROFILE LISTED ABOVE.

ADDITIONAL SCREEN ACCESS (LIST SCREEN ID): (Please provide controls associated with additional screens in the Selective Security Restrictions Section.)

DENIED SCREEN ACCESS (LIST SCREEN ID):

SELECTIVE SECURITY RESTRICTIONS INCLUDE:

Purchasing Module:
 BUYING ENTITIES: _____, _____, _____, _____, _____ and/or FROM: _____ TO: _____

Purchasing/AP Module:
 PAYING ENTITIES: _____, _____, _____, _____, _____ and/or FROM: _____ TO: _____

Procurement Card Module:
 PROCUREMENT CARD: LOCATION CONTROLS _____ CARD NUMBER CONTROLS _____

Inventory Module:
 CATALOG ENTITIES: _____, _____, _____ and/or FROM: _____ TO: _____
 WAREHOUSES: _____, _____, _____ and/or FROM: _____ TO: _____

AR Module:
 AR COMPANY CONTROLS _____, _____, _____, _____, _____, _____, _____ and/or FROM: _____ TO: _____
 AR CREDIT ANALYST CONTROLS _____, _____, _____, _____, _____, _____ and/or FROM: _____ TO: _____

Budgetary Control Module:
 ADD/CHANGE OPERATOR TO **BC DOCUMENT END APPROVAL OPERATOR CONTROL GROUP(S)**:
 _____, _____, _____, _____, _____
(Operator IDs listed for END APPROVAL will have authority to end documents for the Operator ID listed at the top of this form.)

The security request above complies with my agency's internal controls (separation of duties), and policies to prevent security abuses in the NCAS. The operator above has also been given a copy of the OSC personal information disclaimer statement and agrees to comply.

REQUESTED BY: (Agency Security Administrator's Signature) _____ / / (Date)

OSC USE ONLY

CHANGES TO SECURITY COMPLETED BY:
 IF YOU HAVE QUESTIONS ABOUT THIS FORM, CONTACT THE OSC SUPPORT SERVICES CENTER AT (919) 875-4357. REV.: 01/07

NCAS Change Operator Security Profile Form (OSC SEC03) Field Definitions

Selective security restrictions to operator profiles for any NCAS application are defined on the **NCAS Change Operator Security Profile Form, OSC SEC03**. The form is divided into four main sections. The first section is general information to be completed by the agency.

The second section allows the requester to make changes to screen accessibility within the application profile selected for the operator. Therefore, the operator's processing and inquiry capabilities may include access to additional screens not contained in the operator profile and/or profile screens that should be denied.

The third section allows the requester to specify restrictions to screens with more exacting operator controls.

The fourth section is for OSC use only. The operator's security profile can be changed when the agency requests to **ADD** a new operator or make a **CHANGE** to an existing operator.

OPERATOR NAME	Operator's <i>complete</i> name. Always required.
OPERATOR ID #	Operator ID number assigned by the OSC NCAS Security Administration Team. This box should be blank when adding an operator. When changing an operator's access rights, this box should be completed.
AGENCY	Agency name or abbreviation (e.g., Department of Correction or DOC)
AGENCY #	A two-digit OSC assigned agency identifier. (For example, the agency number for DOC is 42.)
REGION	P or NC23. Always required.

CHANGE

APPLICATION*	The application ID is a two-character identifier that represents the application system that the operator will access. The application IDs are listed for the user. One OSC SEC03 form must be completed for each application.
NCAS OR AGENCY PROFILE NUMBER	To change the selected system screens, indicate the NCAS or Agency Security Profile number that will be modified. This is the selected application profile number for that operator.

SCREEN ACCESS

ADDITIONAL SCREEN ACCESS (LIST SCREEN ID)	If the operator's security differs from the selected NCAS or Agency Security Profile, each additional screen ID must be listed. Complete for additional screen privileges that are not granted within the operator's profile assignment.
DENIED SCREEN ACCESS (LIST SCREEN ID)	If the operator's security differs from the selected NCAS or Agency Security Profile, each denied screen ID must be listed. Complete when specific screens are denied.

SECURITY RESTRICTIONS

SELECTIVE SECURITY RESTRICTIONS INCLUDE:

The various system applications have security controls that are set for the selected screens. When changing an operator's application security profile, any differences in the controls for the additional screen IDs must be indicated. These selective security restrictions (controls) must apply for **all** additional screen IDs that were not listed in the previous section. **If selective security restrictions are not specified, the complete agency range is assumed.** If further levels of restrictive security are needed, complete this section.

Purchasing

BUYING ENTITIES	Indicate the appropriate buying entities for the additional screens listed above.
-----------------	---

Purchasing and Accounts Payable

PAYING ENTITIES	Indicate the appropriate paying entities for the additional screens listed above.
-----------------	---

Procurement Card

PROCUREMENT CARD - LOCATION	Indicate the proper controls to secure a cardholder to a particular location or to a particular card.
CONTROLS AND CARD # CONTROLS	

Inventory

CATALOG ENTITIES	Indicate the appropriate catalog entities for the additional screens listed above.
WAREHOUSES	Indicate the appropriate warehouse controls for the additional screens listed above.

Accounts Receivable

A/R COMPANY
CONTROLS

Indicate the appropriate AR company controls for the additional screens listed above.

AR CREDIT ANALYST
CONTROLS

Indicate the appropriate AR credit analyst controls for the additional screens listed above.

Budgetary Control

ADD/CHANGE
OPERATOR BC
DOCUMENT END
APPROVAL OPERATOR
CONTROL GROUPS(S)

Indicate the operator ID that is responsible for approving the BC documents entered by this operator. If the Operator Control Group number is **not** specified, it is assumed this operator can approve his/her own BC documents.

REQUESTED BY

The signature (and date) of the Agency Security Administrator. This signature is **required** when OSC SEC01 is **not** attached.

NCAS INFORMATION EXPERT SECURITY REQUEST FORM

OSC FORM SEC04

OPERATOR NAME: _____	OPERATOR ID #: <input style="width: 100%;" type="text"/>
-----------------------------	---

- IF REQUESTING AN OPERATOR ID FOR APPLICATION AND I.E. ACCESS, **COMPLETE OSC SEC01 AND OSC SEC04 FORMS.**
- IF REQUESTING AN OPERATOR ID FOR I.E. ACCESS **ONLY**, **COMPLETE OSC SEC04 FORM.**
- IF REQUESTING A **CHANGE** TO I.E. ACCESS OR IF **DELETING** I.E. ACCESS, **COMPLETE OSC SEC04 FORM.**

COMPLETE THIS SECTION WHEN REQUESTING AN OPERATOR ID FOR I.E. ACCESS ONLY OR WHEN CHANGING OR DELETING I.E. ACCESS:

TYPE OF REQUEST: <input style="width: 30px; height: 20px;" type="checkbox"/>	A = ADD I.E. ACCESS	C = CHANGE I.E. ACCESS	D = DELETE I.E. ACCESS
AGENCY: _____ AGENCY #: _____ REGION: _____		ORG: _____	
		RACF ID: _____ RACF GROUP: _____	
OPERATOR'S JOB TITLE AND DESCRIPTION: _____ _____			

COMPLETE THIS SECTION WHEN REQUESTING OR CHANGING I.E. ACCESS:

The operator will:	
<input type="checkbox"/>	Provide technical support to your agency through I.E.
<input type="checkbox"/>	Only run I.E. reports found in Public Libraries.
<input type="checkbox"/>	Create new I.E. reports and run I.E. reports found in Public Libraries.
Preferred Default IE Library:	
<input type="checkbox"/>	Financial (Finan)
<input type="checkbox"/>	Miscellaneous (Misc)
<input type="checkbox"/>	Management (Mtmgt)
<input type="checkbox"/>	User
Preferred Technical Library	
<input type="checkbox"/>	DP
<input type="checkbox"/>	Production
The operator above has been given a copy of the OSC personal information disclaimer statement and agrees to comply.	
REQUESTED BY: _____	____ / ____ / ____ (Date)
<i>(Agency Security Administrator's Signature)</i>	

OSC USE ONLY

OPERATOR ID #: <input style="width: 100%;" type="text"/>	INITIAL PASSWORD: _____
I.E. GROUP: _____	I.E. DEFAULT LIBRARY: _____
I.E. SECURITY COMPLETED BY: _____	
<i>(I.E. Security Administrator's Signature)</i>	
____ / ____ / ____ (Date)	

IF YOU HAVE QUESTIONS ABOUT THIS FORM, CONTACT THE OSC SUPPORT SERVICES CENTER AT (919) 875-HELP. REVISED: 03/06

NCAS Information Expert Security Request Form (OSC SEC04) Field Definitions

I.E. security allows certain operators reporting capabilities. I.E. restrictions for an operator are defined on the **NCAS Information Expert Security Request Form, OSC SEC04**. This form is divided into two main sections. The first section is completed by the agency. It is divided into three areas. The second gray section is for OSC use only.

The second area allows the requester to designate the **Type of Request** and to provide additional general information about the requesting agency and the operator. The **Type of Request** must always be completed. If the requester has completed OSC SEC01, the general information may be omitted on OSC SEC04.

The requester must **always** complete the third area when requesting an **ADD** operator or a **CHANGE** to an operator. Completion of this area determines the operator's primary I.E. responsibilities and which I.E. libraries the OSC NCAS I.E. Security Administrator should assign to the operator.

If the Agency Security Administrator is requesting application security and I.E. access for a new operator, he or she should complete security forms OSC SEC01 and OSC SEC04. If the Agency Security Administrator is requesting I.E. access **only** for a new operator, a change to an operator's I.E. access, or the deletion of an operator's I.E. access, he or she should complete OSC SEC04.

OPERATOR NAME	Operator's <i>complete</i> name. Always required.
OPERATOR ID #	Operator ID number assigned by the OSC NCAS Security Administration Team. This box should be left blank when adding an operator. It is required when changing or deleting an operator's access rights.
TYPE OF REQUEST	Indicate the type of security request: A = Add Operator = Add a new operator to the NCAS I.E. System C = Change Operator = Change an existing operator's I.E. security D = Delete Operator = Delete an existing operator from the NCAS I.E. System Always required.
AGENCY	Agency name or abbreviation (Department of Correction or DOC). This is required if the type of request is a CHANGE or a DELETE operator I.E. access or an OSC SEC01 form has not been completed.
AGENCY #	A two-digit OSC assigned agency identifier. (For example, the agency number for DOC is 42.) This is required if the type of request is a CHANGE or a DELETE operator I.E. access or an OSC SEC01 form has not been completed.

REGION	P or NC23. Always required.
ORG	<p>ORG is a 20-byte alphanumeric user-defined field. The agency may use the ORG field for its own internal reporting requirements. Because the ORG field is the secondary sort for security reports, it is the agency's responsibility to maintain this field and define each operator within the agency's internal structure.</p> <p>If an agency has divisional locations, the ORG field may identify the agency's department or division location for the operator. (For example, a DOC operator may be located at the Division of Prisons.)</p> <p>The ORG field may represent a further breakdown of the agency's internal organizational structure. In this case, the ORG field is similar to the NCAS Responsibility Cost Center (RCC). The agency may designate a valid structure that represents its organization and is a logical basis for grouping NCAS operators within the agency. Some agencies select the data elements located somewhere in positions six (6) through twelve (12) of the General Ledger Center. Other agencies may select positions one (1) through four (4).</p>
RACF ID	Mainframe system access is defined to Resource Access Control Facility (RACF) and assigned to the operator by the Agency Security Administrator. This is required if the type of request is a CHANGE or a DELETE operator I.E. access or if an OSC SEC01 form has not been completed.
RACF GROUP	The RACF ID is defined to a RACF Group by the Agency Security Administrator. This is required if the type of request is a CHANGE or a DELETE operator I.E. access or if an OSC SEC01 form has not been completed.
OPERATOR'S JOB TITLE AND DESCRIPTION	A brief description of the operator's job functions. For example, Accounts Payable Processor may describe an operator's job and related duties. This is required if the type of request is a CHANGE or a DELETE operator I.E. access or if an OSC SEC01 form has not been completed.

OPERATOR RESPONSIBILITIES DEFAULT I.E. LIBRARIES

THE OPERATOR WILL The requester should check the appropriate box. This is **required** if the type of request is an **ADD** operator I.E. access or a **CHANGE** operator I.E. access.

OPTION 1: Technical support: Operator assigned to MIS group

OPTION 2: Functional or technical: Operator assigned to agency group

OPTION 3: Functional or technical operator who develops I.E. reports: Operator assigned to agency group

THE OPERATOR WILL The requester should check the appropriate box. This is **required** if the type of request is an **ADD** operator PRIMARILY RUN I.E. access or a **CHANGE** operator I.E. access. **Mark at least one.**

If *Option 1* in the above section is checked, the default I.E. library is DPXX (where XX is the agency number).

If *Option 3* in the above section is checked, the default I.E. library is USERXX (where XX is the agency number).

If *Options 1 and 3* in the above section are **not** checked and:

- Line 1 is checked, the default I.E. library is FINANXX (where XX is the agency number).

- Line 2 is checked, the default I.E. library is MTMGTX (where XX is the agency number).

- Line 3 is checked, the default I.E. library is MISCXX (where XX is the agency number).

- Line 4 is checked, the default I.E. library is ADMINXX (where XX is the agency number.)

The libraries are maintained by the agency's I.E. Security Administrator. This person should have access to TSO and a good knowledge of JCL. The users can copy RUN-STATEMENTS from the Public Libraries into their default libraries before submitting the reports. Because these are shared libraries, it should never be assumed that any member is as a user last left it. Always check the RUN-STATEMENTS before submitting a job. The RUN-JCL should also be checked to ensure that the correct files are being read and that the reports will be printed on the correct printer.

ADMINIXX Only run I.E. reports found in Public Libraries

DPXX Used by the MIS staff for development of agency-specific reports. The reports can be moved to other libraries for reporting.

FINANXX Established for users who primarily run financial (GL, FC, and BC) reports.

MISCXX Established for users who primarily run AR or FA reports.

MTMGTXX Established for users who primarily run materials management (AP, PS, and IN) reports.

PRODXX Used for production reporting. Access is restricted to MIS staff.

USERXX Used by the Non-technical staff for development of agency-specific reports.

REQUESTED BY

The signature (and date) of the Agency Security Administrator. This signature is **required** when OSC SEC01 is **not** attached.

OSC USE ONLY

OPERATOR ID #

Operator ID number assigned by OSC NCAS Security Administration Team.

INITIAL PASSWORD

The initial password in an **ADD** request will **always** be the employee's first name and the agency's ID number.

I.E. GROUP

I.E. group is assigned by the OSC NCAS I.E. Security Administrator.

I.E. DEFAULT LIBRARY

I.E. Default Library is assigned by the OSC NCAS I.E. Security Administrator.

I.E. SECURITY COM-
PLETED BY

When the I.E. security has been completed, the OSC NCAS I.E. Security Administrator stamps the form with the date of completion and the position number of the employee processing the request.

NCAS Security Reports

```
X 1 V22: Favorites                               Found
Command ==>                                     Scroll ==> CSR

Commands: PRO - Update Favorites (via Profile)
Options:  B - Display on terminal      X - List report indices
          S - List report versions    V - List report views
          PRT - Print                  Q - Add to Work Queue
          SQ - Structured Query        N - Version Notes
Use END command to exit. Use LEFT command to list more report information.

Opt  Type  Title                                          Last CMD
RPT  OSCOPC SECURITY PROFILE REPORT
RPT  OSCOPC SECURITY REPORTS/ AGENCY
RPT  OSCOPC SECURITY REPORTS/ AP
RPT  OSCOPC SECURITY REPORTS/ AR
RPT  OSCOPC SECURITY REPORTS/ BC
RPT  OSCOPC SECURITY REPORTS/ FA
RPT  OSCOPC SECURITY REPORTS/ FC
RPT  OSCOPC SECURITY REPORTS/ GL
RPT  OSCOPC SECURITY REPORTS/ IN
RPT  OSCOPC SECURITY REPORTS/ OSC
RPT  OSCOPC SECURITY REPORTS/ PC
RPT  OSCOPC SECURITY REPORTS/ PS
RPT  OSCOPC SECURITY REPORTS/ PT
```

The NCAS Security Reports are executed and spooled to the Systemware (X/PTR) during the weekly production process. The NCAS Security Reports are executed once a week. The Agency Security Administrator should view the security reports, verify that each security request has been correctly completed, and notify the OSC NCAS Security Administration Team of any discrepancies. Only Agency Security Administrators are secured to an X/PTR security RACF group and can view the agency's security reports. The security reports or a portion(s) of the security reports may be selected and printed using the X/PTR print utility, and routed to the agency host printer.

The NCAS Security Reports are located in X/PTR under the menu selections:

- OSCO* SECURITY REPORTS/AGENCY
- OSCO* SECURITY REPORTS/AP
- OSCO* SECURITY REPORTS/AR
- OSCO* SECURITY REPORTS/BC
- OSCO* SECURITY REPORTS/FA
- OSCO* SECURITY REPORTS/FC
- OSCO* SECURITY REPORTS/GL
- OSCO* SECURITY REPORTS/IN
- OSCO* SECURITY REPORTS/PC
- OSCO* SECURITY REPORTS/PS
- OSCO* SECURITY TABLE UPDATE OSC
- OSCO* SECURITY USERS TABLE LIST



An asterisk (*) in the job/group name represents a region-specific variable. Use **C** to reference report groups in the SCCP region. Use **F** to reference report groups in the NC23 region.

NCAS Agency Security Reports

The NCAS Agency Security Reports comprise an X/PTR report series that provides a detailed listing of an operator's application security profile data. They present the relationship of controls to screen functions within any given application for each operator.

The NCAS Agency Security Reports series are comprised of two reports. The Operator/Function Cross-Reference Report (S0001) lists the availability of each screen function for an operator within an application. The Operator/Secured keys Cross-Reference Report (S0003) lists all screens that are secured to specific controls within an application. Each report includes the operator's name and the NCAS Operator ID number.

The NCAS Agency Security Reports are sorted as follows:

- Agency Number
- Agency Sort (Organization)
- Alphabetically by Operator Last Name
- NCAS Application
- Operator/Function Cross-Reference (S0001)
- Operator/Secured Keys Cross-Reference (S0003)

The X/PTR report distribution is as follows:

Report ID	XX-S0001 (where XX represents an application)
Report Name	Operator/Function Cross-Reference
X/PTR Report Series	OS COP* SECURITY REPORTS/AGENCY

Report ID	XX-S0003 (where XX represents an application)
Report Name	Operator/Secured Keys Cross-Reference
X/PTR Report Series	OS COP* SECURITY REPORTS/AGENCY

NCAS Application Security Reports

The NCAS Application Security Reports comprise an X/PTR report series by application that provides a detailed listing of an operator's security profile data. Each X/PTR application selection has a set of three reports. In addition to the Operator/Function Cross-Reference Report (S0001) and Operator/Security Keys Cross-Reference Report (S0003), the Function/Operator Cross-Reference Report (S0002) is provided. In a triple columnar format, the Function/Operator Cross-Reference Report (S0002) alphabetically lists all operators within an agency that are allowed access to a screen in any given application. The corresponding NCAS Operator ID number is listed for each operator.

The NCAS Application Security Reports are sorted as follows for each application:

- Operator/Function Cross-Reference (S0001)
 - Agency Number
 - Agency Sort (Organization)
 - Alphabetically by Operator Last Name

Function/Operator Cross-Reference (S0002)

Agency Number
Agency Sort (Organization)
Function Code (Screen)
Alphabetically by Operator Last Name

Operator/Secured Keys Cross-Reference (S0003)

Agency Number
Agency Sort (Organization)
Alphabetically by Operator Last Name

The X/PTR report distribution is as follows:

Report ID	XX-S0001 (where XX represents an application)
Report Name	Operator/Function Cross-Reference
X/PTR Report Series	OSCOPI* SECURITY REPORTS/XX (where XX represents an application)

Report ID	XX-S0002 (where XX represents an application)
Report Name	Function/Operator Cross-Reference
X/PTR Report Series	OSCOPI* SECURITY REPORTS/XX (where XX represents an application)

Report ID	XX-S0003 (where XX represents an application)
Report Name	Operator/Secured Keys Cross-Reference
X/PTR Report Series	OSCOPI* SECURITY REPORTS/XX (where XX represents an application)

DCI User File Reports

List of DCI Users Security Reports

The List of DCI Users Security Reports comprise an X/PTR report series that provides additional operator information not located in DCI security. The List of DCI Users Security Reports is comprised of three reports. Each of the three reports contains the same information with different sorts. The first report is sorted by the NCAS Operator ID numbers within an agency. The second report is alphabetically sorted by the operators' last names within an agency. The third report is sorted by the operators' RACF ID numbers within an agency.

These security reports are executed after all security maintenance jobs are complete. The NCAS Operator ID number and the alphabetical listings are spooled to X/PTR with a printed distribution to the OSC NCAS Security Administration Team. At this time, the Employee ID number is replaced with blanks in the reporting format.

The following operator information is contained in each report:

- NCAS Operator ID Number
- Agency Number
- Employee ID Number
- Agency Sort (Organization)
- Operator Name
- RACF ID Number
- Date of Maintenance
- I.E. Indicator

The X/PTR Report distribution is as follows:

Report Name	List of DCI Users by Agency/Operator ID
X/PTR Report	OSCOPT* SECURITY USERS TABLE LIST
Report Name	List of DCI Users by Agency/Alphabetical
X/PTR Report	OSCOPT* SECURITY USERS TABLE LIST
Report Name	List of DCI Users by Agency / RACF ID
X/PTR Report	OSCOPT* SECURITY USERS TABLE LIST

DCI User Files

The DCI User Table Maintenance Reports is a X/PTR report series that identifies OSC DCI User Table maintenance.

DCI User Table OSC Maintenance Reports

The DCI User Table OSC Maintenance Reports comprise an X/PTR report series for OSC maintenance transactions. The OSC NCAS Security Administration Team uses the DCI User Table OSC Maintenance Report to verify DCI User File maintenance. The DCI User Table OSC Maintenance Report provides a list of NCAS operator ID numbers that were added, changed, or deleted during the weekly update. The OSC NCAS Security Administration Team enters these additions, changes, and/or deletions to the DCI User File via a TSO data set.

The DCI User Table OSC Maintenance Report is a weekly notification to agencies that the OSC NCAS Security Administration Team has performed the security updates. The Agency Security Administrators should verify that all security requests were processed. The detail DCI security information for an operator can be found in the NCAS Agency Security Reports or the NCAS Application Security Reports.

The X/PTR report distribution is as follows:

OSC DCI User Table Maintenance

Report Name'	DCI User Table Maintenance
X/PTR Report Series	OSCO* SECURITY TABLE UPDATE OSC

Using the NCAS Information Guide (SIG) to Access Security Profiles

1. Open your Internet browser.
2. Type **http://www.ncosc.net** for the address of the OSC's web page.
3. Click the **System Information Guide** link under the NC Accounting System section.
 Bookmark this location for future use.
4. Click the **Security Profiles** link under the Documentation section.
5. Click the type of Security Profile you would like to view.
6. Click the module you would like to view.
7. Click the profile type you would like to view.

NCAS Password Security

NCAS Security Upgrade

The OSC is enhancing password security in the North Carolina Accounting System (NCAS). All NCAS users currently have an operator id and password to log into NCAS. The following password requirements will be in effect beginning **November 17, 2008**:

- **90 Day Password Expiration Period:** NCAS users are required to change their password every 90 days.
- **Seven Day Password Warning Period:** A warning message is displayed within the NCAS system. Beginning on the seventh day prior to password expiration, the user will begin receiving messages that read "YOUR PASSWORD WILL EXPIRE IN # DAY". If the password is not changed within seven days of the initial warning, the operator id status will become **EXPIRED**.
- **90 Day Inactivity Period:** If an NCAS user fails to successfully log in during a 90 day period, the operator id status will become **INACTIVE**.
- **Three Failed Login Attempts:** if an NCAS user attempts to log in and is unsuccessful in three consecutive attempts in one session, the NCAS system operator id status will become **REVOKED**.
- **Password Resets:** If an operator id becomes Revoked, Expired or Inactive, the agency NCAS Security Administrator must contact OSC Support Services at (919) 875-HELP (4357) to have the password reset. Support Services will assign a temporary password and change the operator id status to **EXPIRED**. Once the password is reset, the NCAS user will be required to change their password during their next sign-on attempt.

10/10/08

