



OFFICE OF STUDENT FINANCIAL ASSISTANCE GUIDE TO INFORMATION SECURITY AND PRIVACY

This Guide is For Everyone

All Student Financial Assistance (SFA) employees, partners, and contractors need to understand how to protect their resources and customers' privacy. This guide provides you with a clear and concise view of the existing Department of Education Information Security Policy and how it relates to SFA. It also outlines the necessary procedures you should use to minimize risks and to make sure SFA systems are available when SFA customers and partners need them.



We help put America through school...securely!



Why This Guide Applies to You

If you use a computer system, you are accepting security risks. Each time you choose to open an email attachment or load material from a floppy disk, you are accepting risks. You must accept these risks because nothing in our world of interconnected computer networks is free of security risks. As part of the SFA commitment to improved customer service, reduced unit costs, and improved employee satisfaction, we are all responsible for managing these risks. Commitment to information security protects our customers' privacy, avoids fraud, and builds confidence in our partners and in the public.

Without effective security practices, a single employee can have a devastating impact on the entire SFA organization. As was seen recently with the "I Love You Virus," a single person inside SFA can unknowingly launch a hostile program attached to an email that erases data, causes servers to crash, and interrupts information flow with our customers.

What Threats Face SFA?

Security is about managing risks, and that means understanding the threats that cause these risks. Threats jeopardize two vital parts of the student aid delivery system: (1) our **Internal** SFA systems, (including both the hardware and software that make up these systems, and the data they contain) and (2) our **Partners'** systems.

Threats fall into three major categories:

- *Confidentiality* – Information must be protected from unauthorized disclosure;
- *Data Integrity* – Information must be reliable, therefore accurate; and
- *Availability* – Information and systems must be accessible when needed.

These three fundamental Computer Security concerns are often referred to as **CIA**: **confidentiality, integrity, and availability**.

Confidentiality risks arise from the failure to keep SFA information private and the failure to limit access to authorized individuals only. Let's view this in the context



of one of our customers ... the student applying for aid using the Free Application for Federal Student Aid (FAFSA), either on the Web or via the traditional paper application. The student is required to enter sensitive information, which includes home address, income (or parents' income), and driver's license number. Once the student completes and signs the form (which may include parental signature), data from the form are entered into the Central Processing System. Along the way, SFA contractors have access to information that our student probably doesn't want shared. Some of the contractor's personnel have a **need to know**

but others do not. Keeping private information private is one of the central promises we and our partners make to our customers.

Integrity risks deal with accuracy of data. We minimize these risks by making sure data stored in SFA systems is protected from improper changes. Let's go back to our FAFSA example. What if someone unilaterally changes the student's income and family size? These changes would have an impact on that student's aid eligibility. To protect against this, the application processing system has built-in **Integrity** checks to ensure data accuracy.

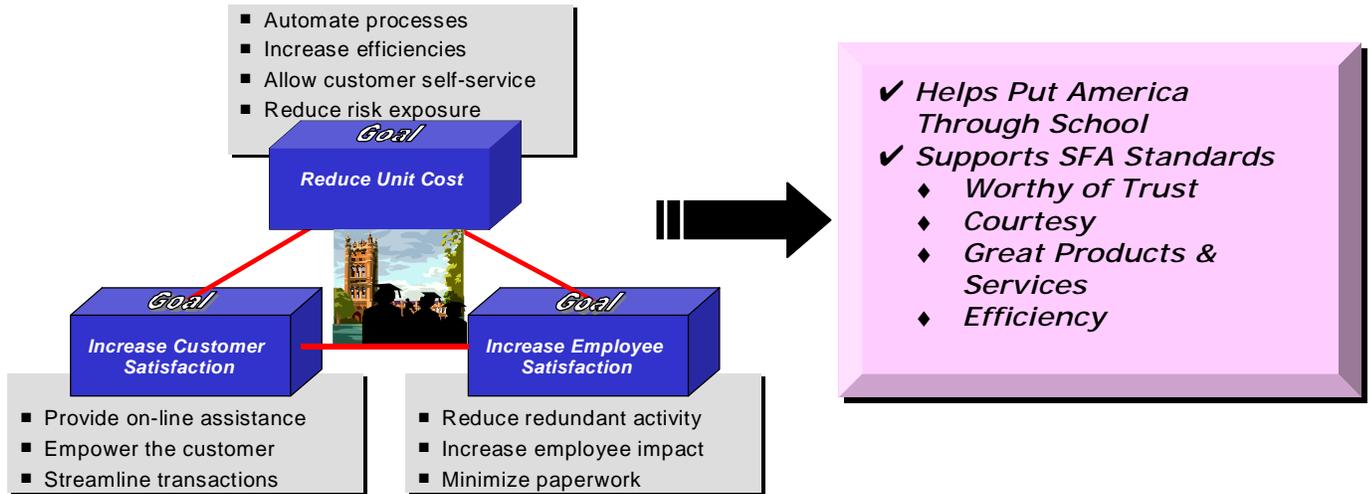


Availability risks are the risks that SFA systems may not be available to our customers, partners and users when they need them. Systems may become unavailable due to viruses, hacker attacks, improper system changes, or failures in the supporting infrastructure (power, communications, etc.).

Again, returning to our FAFSA example, let's suppose that a customer wants to submit her FAFSA application via the web. Knowing that the electronic FAFSA was available, she waited until the last minute to complete it. If the FAFSA web site is unavailable she will be unable to submit her application on time. *System outage equals customer outrage!*

We protect SFA systems, information and resources against threats from inside and outside by insisting on comprehensive system security plans, by training our staff and our contractors, and by protecting student / borrower private information at all times. We also help our partners protect their systems and customer data by requiring good computer security practices throughout the student aid industry.

Security management lets SFA achieve its goals of reducing operating costs, increasing customer satisfaction, and improving employee satisfaction. Successful security practices let customers achieve their education goals. Our customers should always be at the center -- each goal must be achieved while meeting our customers' service expectations.



What Can You Do?

As an SFA employee, your responsibility is simple: prevent the theft, destruction, and unauthorized access of SFA data and systems!!

This sounds like an impossible job for a single employee, but all employees working together can make it happen. For example, though you need to make sure your own data is backed up and stored safely, you can rest assured that the mass of data we maintain on schools, borrowers and financial institutions is backed up every day. And someone is making sure a well-managed firewall is protecting your desktop computer from rogue Internet connections.

Learning your part in SFA information security and privacy protection begins by identifying your role in SFA. This guide is organized around employee / contractor roles and the types of security on which those in each role should focus.

How to Use This Guide

The guide is divided into four sections, corresponding to security-related roles in SFA:



End Users



Security Managers



Systems



Acquisition

You may play more than one role, but at minimum, everyone is an SFA systems user.

1. **End Users** – Those who use SFA information technology (IT) systems and / or have access to customer and partner information. *We are all members of this category!*
2. **Security Managers** – Those responsible for proper operation of IT systems and development of security policy and controls.
3. **Systems** – Those responsible for daily operating, maintaining, and configuring SFA IT resources, and for developing and testing applications or software.
4. **Acquisition** – Those involved with procuring IT services or equipment.

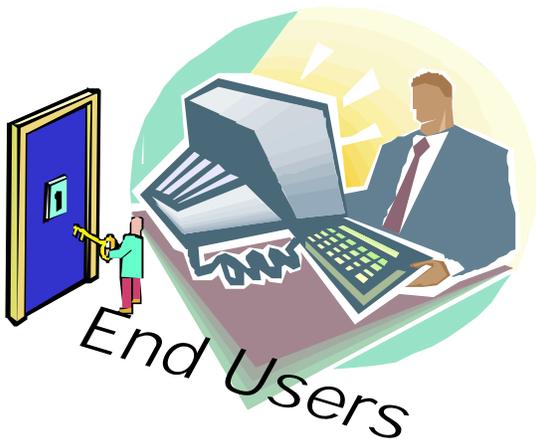
In addition, Section II of this guide explains the requirements of OMB Circular A-130, which defines the government-wide policy on information systems security.

The SFA mission is to “Help Put America Through School” and successful computer security practices will help us achieve this goal. Security and privacy protection are critical factors by which both your success and SFA's success will be measured. You must actively support a secure operating environment by learning the existing policy, practicing what you have learned and teaching others every day.



* Think - Do - Teach *
Unlock Your Potential

RESPONSIBILITIES OF END USERS



DESCRIPTION:

"Welcome to SFA! You're now one of the biggest keys to securing SFA information systems and privacy data in the whole organization."

OK, maybe that's a bit drastic, but the point is that no security policy will be successful unless every user participates. Everyone working together creates a solid barrier to repel would-be thieves. Each user supports a specific area of this shield, and is in turn supported by the other users. Holes in this barrier create vulnerabilities for criminals to exploit.

With our increasing dependence on networked computer systems and exchange of information via the Internet, security lapses can translate into millions of dollars of lost productivity and stolen assets. Security failures can also affect SFA's ability to perform its mission and your ability to do your job.

Security is not another whim or trend that will be tacked on the office bulletin board ... no more than locking the door on your house is a response to advertising by the lock industry. Securing and protecting SFA information and systems should become a part of everyone's daily

routine. And it's not just SFA saying this. Every Government organization is under enormous pressure to meet to the highest security standards.

The Internet has improved your ability to share information among student aid organizations. But this improved connectivity brings increased risks because the **access** needed to share information is the same access used by hackers and thieves to penetrate systems, disrupt operations, steal privacy information and commit fraud. Increased risk requires better security awareness and knowledge among SFA employees.

OK, enough of the scary stuff. Before we start with your specific "SFA user things to do," let's look at other areas, which are a part of your everyday life, where **you** have a personal stake in the **privacy** and **security** of information:

- **Banking** - Writing a check, withdrawing money from an ATM, or applying for a loan.
- **Life Insurance** - Disclosing medical history, income, and life habits.
- **Online Purchases** - Providing credit card numbers, mailing addresses, and personal profiles.

And the list goes on ... school transcripts, medical records, legal records, mortgage paperwork ...

In all these transactions, you rely on industry to provide the right kind of security to protect your information. Our customers count on users like you to protect the information they entrust to SFA. You're the one responsible for following SFA policies and procedures to secure our information systems and sensitive information.

Let's now readdress the three fundamental computer security concerns: **confidentiality**, **integrity**, and **availability** ... or *CIA*.

As a user, all three of these concerns have significant implications for you. A failure in any computer security area may prevent you from completing your job, or expose you and SFA to liabilities. As users, few are able to impact the *integrity* or *availability* of SFA systems. However, in the area of *confidentiality*, a user can have a direct impact. By protecting your user ID and password, concealing applicant or borrower private information, and properly disposing of sensitive data, users are the front line of defense against those interested in exploiting SFA information.

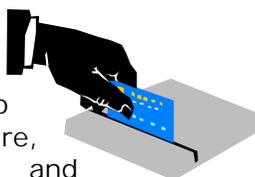
What does it take to operate SFA systems securely? Briefly, it's the daily use and support of sound security practices and methods. It is useful to think about user security responsibilities under four headings:

- Administrative Security
- Personnel Security
- Physical Security
- Information Security

Administrative Security accounts for your identity and your access to the systems. It also considers your job responsibilities and how security relates to your activities.

Personnel Security addresses background checks and security clearances. The end goal is to make sure you are worthy of the trust and responsibility of the SFA position to which you are assigned.

Physical Security focuses on protecting information assets, to include hardware, software, information and



people. Within this area lie the physical controls that monitor access to SFA locations and **control areas**. Typical physical controls are locks, keypad entry systems, photo identification / card readers, and security guards. An SFA computer user needs to submit requests for the appropriate physical security credentials based on job location and description. You should also check with your supervisor to confirm your physical access privileges.

Another major component in this area is Disaster Recovery Plans. These plans will help you respond to any physical damage SFA resources may experience. You should understand your role in any Disaster Recovery, Contingency, or Continuity of Operations Plan.

Information Security is the provision and maintenance of user IDs, passwords, privileges, and specific system security training. For the user, information security is about the proper handling of your ID and password to include protecting and changing them as required. You need to make sure you can access the systems you use with the privileges needed to do your job.

Your ID and passwords are unique to you and are used to track your activities as you use any SFA system. (This should help you think twice before you share your unique identity with someone else!) Sharing your personal access codes is prohibited.

You will receive system privileges based on what you require to do your job. Privileges are controlled this way to keep them at the lowest level necessary to complete the job.

Computer security is a learned skill, and SFA users have several opportunities to attend security training. The first of these is security

awareness training. Each new SFA employee is required to attend this training within 30 days of hire. Additionally, all SFA employees must get security awareness training once per year. System training provides you with the necessary knowledge to operate the system to complete your job. During this training, you will learn:

- The security features built into the applications and information systems.
- How to recognize a security incident and how to respond to one.
- How to access, process and handle sensitive information.
- How to dispose of sensitive information properly.
- The specifics of your Disaster Recovery, Contingency and Continuity of Operations Plans, and how they impact you as a user.

It should be clear that security is a fundamental part of your daily job. The following **To Do** list will identify many of the essentials. In addition, it will point out many of the things you will need to learn to contribute to SFA security and program success.



THINGS TO DO:

- ❑ **Complete** and submit your security paperwork
- ❑ **Attend** Security Awareness Training within 30 days of taking a new position
- ❑ **Mark, control, and store** all media properly

- ❑ **Stay alert** to your physical environment; report any abnormal packages, email, or activity immediately
- ❑ **Request** system access through the appropriate administrator
- ❑ **Change** passwords in accordance with instructions, more frequent is better
- ❑ **Never** share or write down passwords (this includes notes underneath your keyboard or on your monitor)
- ❑ **Never** leave logged-in systems unattended / unsecured (log off before leaving your workstation)
- ❑ **Attend** system-specific training to learn special security features
- ❑ **Never** load your own software, to include unauthorized Internet downloads. Ask a system administrator to obtain and load new software for you
- ❑ **Protect** remote access (dial-in) phone numbers and information
- ❑ **Know** what represents a security or privacy breach
- ❑ **Know** the proper security official to whom you should report security incidents
- ❑ **Report** all security breaches to the proper person
- ❑ **Learn** what sensitive information you have access to, and proper information-handling procedures
- ❑ **Clear** your work area of sensitive information when you are not there



- ❑ **Dispose** of sensitive information properly
- ❑ **Review** Disaster Recovery, Contingency and Continuity of Operations Plans that impact you and your assigned information systems and understand your role in the execution of those plans

RESPONSIBILITIES OF SECURITY MANAGERS



DESCRIPTION:

Congratulations! Your hard work has earned you a security management position. Of course, the big challenge now is to master the various aspects of your new position. This section will answer the specifics of what you, as a manager, should do in the realm of security and privacy.

Although each of us is responsible for success of the SFA security program, those in security management are accountable for *implementation and administration* of security. Management functions include identifying and designating specific security roles and responsibilities, creating and maintaining security policy and plans, certifying and accrediting information systems, integrating security information into business processes and SFA security objectives, and identifying training requirements.

The following are brief descriptions of SFA Security Managers and their roles:

- SFA Chief Operating Officer (COO)
- Responsible for protecting IT resources within SFA, establishing policy and directives, and directing implementation of security practices.

- Computer Security Officer (CSO) – Implements and maintains the Information Technology Security Program within SFA. Advises SFA Management Council. Coordinates security policy and directives and supports the SPAs and SSOs. Works closely with Department of Education security officials.
- Functional Manager (FM) - Top-level SFA managers with one or more IT systems under their control. Includes General Managers, Ombudsman, CFO and CIO. Responsible for information systems within their respective areas, and for establishing, maintaining, and enforcing computer security policy.
- Security and Privacy Advocate (SPA) - Serves as security and privacy advisor to an FM. Works with SMs and SSOs to develop and implement security policy and procedures within a functional area. Stays current on security and privacy related events, keeps current on security training, and helps to disseminate policy originating from the CSO.
- System Manager (SM) - Supervises the daily operation and maintenance of a specific information system. Manages personnel, system operations, and interoperability with other systems. Coordinates the efforts of administrators (systems, network, and database), system maintenance personnel, and system programmers. Certifies system to FM as secure and ready for operation. Relies on System Security Officer.
- System Security Officer (SSO) - Designated by the FM or equivalent, the SSO implements SFA's security policy in a specific information system. Responsible

for protection and privacy of information processed or stored in that system. Serves as the focal point for the physical security of the system. Works with SM and SPA.

- Data Owner - Responsible for the accuracy, confidentiality and availability of the data in a specific information system. In SFA, FMs are data owners for systems they control.

All these positions work together to implement a security program to protect SFA information assets.

Those in security management should also concern themselves with the four types of security: Administrative, Personnel, Physical, and Information.

For security managers, the bulk of **Administrative** security effort focuses on documenting security policy, procedures and organization. This documentation takes the form of designation letters, organization charts, policy and procedure documents, process flow charts and test plans.



Personnel Security

focuses on the process to get employees cleared to perform their jobs. As management, you are responsible for determining the necessary clearance level based on sensitivity of the data being accessed. Based on the employee's role, you'll decide whether a simple background check is sufficient, or if a more in-depth clearance is necessary. Additionally, you must determine the appropriate access level for each position accessing the information system. Clearance levels and control procedures are usually documented in a system's security plan.

Your next challenge is determining the **Physical** security controls necessary to protect SFA assets. These controls can be as simple as locks on doors, or as extreme as biometric access devices. An additional safeguard is identifying **control areas** for special security consideration. Control areas are physical locations that house some part of an information system critical to its operation. Examples may be the network switches that control communications or the machine that houses sensitive information. Control areas must be designated in writing by the System Manager, and given special consideration for physical security protection.

In all these areas, the burden is on you to determine appropriate security measures and to document them in your system security plan. What constitutes appropriate security measures? Check with the rest of the management team, or request assistance from outside security practitioners.

Information Security concentrates on technical activities needed to protect the data, application and communication resources that make up an information system.

Many of the most important information security efforts are carried out by those being supervised by security management personnel. But management is responsible for seeing that such steps as configuration control, disciplined testing, etc., are carried out.

Management must work toward prudently implementing security to support SFA operations and employees. Some of these implementations include establishing configuration control and change management processes to protect the integrity of system operations, and restricting certain functionality based

on user roles. Security management can be simplified through using automated tools. Centralized, role-based access control is an excellent first step toward effective enterprise-wide access control.

The following **To Do** list outlines specific actions required of various Security Management practitioners.



THINGS TO DO:

SFA Chief Operating Officer (COO)

- ❑ **Maintain** overall responsibility for securing SFA data and information systems.
- ❑ **Establish** and **review** changes to SFA security policy by appointing a Computer Security Officer (CSO) as the SFA security advocate
- ❑ **Create** the Information Security and Privacy Working Group and implement recommendations as necessary
- ❑ **Encourage** Department of Education and extra-Departmental (GAO, OMB, etc.) participation

Computer Security Officer (CSO)

- ❑ **Review** Department of Education policy and incorporate it into SFA policy
- ❑ **Issue** designation letters identifying FMs, Data Owners, Designated Accreditation Authorities (DAAs), SPAs, and Certifying Officials (COs)
- ❑ **Appoint** primary points of contact for security incidents

- ❑ **Meet** regularly with Department and SFA security officials
- ❑ **Document** and maintain security standards for new hardware or information systems which operate on Departmental networks
- ❑ **Maintain** records of all systems' Disaster Recovery, Contingency and Continuity of Operations Plans
- ❑ **Review** and **track** the existence of effective Disaster Recovery, Contingency, and Continuity of Operations Plans for each information technology installation and system within SFA
- ❑ **Make sure** physical security requirements are met for each SFA information technology installation and system via coordination with SSOs
- ❑ **Establish** and **enforce** policies on the introduction and removal of hardware/software into and from SFA systems and facilities

Functional Manager (FM)

Note: Some of the duties below belong to the FM because, unless otherwise designated, the FM is the Data Owner and Designated Accrediting Authority for systems under their control.

- ❑ In role as the DAA, **accredit**, no less frequently than every three years, each assigned system as authorized to operate. The three options are:
 - (1) Unconditional Accreditation,
 - (2) Conditional Accreditation, or
 - (3) Refuse Accreditation.

Accreditation must be at a level equal to or more restraining than the system certification

- ❑ **Designate** a System Security Officer (SSO) for each information system
- ❑ **Appoint** a SPA
- ❑ **Hold** SSOs, SMs and SPAs accountable for assigned security duties
- ❑ **Make sure** staff follow training regimen
- ❑ **Make sure** staff follow screening procedures for system access requests
- ❑ **Make sure** detailed position descriptions define responsibilities and system privileges
- ❑ **Implement** configuration and change management controls to make sure new system implementations are approved, tested and user-accepted before operation
- ❑ **Make sure** no SFA technology resource is connected to a network that does not provide adequate protection
- ❑ In role as Data Owner, **Establish** data elements designated as sensitive information

Security and Privacy Advocate (SPA)

- ❑ **Provide advice and counsel** to the FM, SSOs and System Managers in all security and privacy matters
- ❑ **Review** current events, training notices, and impacting policy and disseminate to the organization
- ❑ **Coordinate** closely with the CSO to identify issues, define solutions, and monitor progress

- ❑ **Participate** in SFA-sponsored security and privacy working groups
- ❑ **Conduct** system reviews for Certification and Accreditation and advise the FM

System Security Officer (SSO)

- ❑ **Monitor** daily operations of assigned system and report anomalies to CSO
- ❑ **Determine** appropriate security requirements for assigned system
- ❑ **Develop** and **implement** access lists to controlled areas and information systems for individual users based on name and position
- ❑ **Make sure** necessary physical security is in place to protect system assets
- ❑ **Advise** System Manager on identifying controlled areas
- ❑ **Authorize** movement of equipment into or out of controlled areas
- ❑ **Develop** escort procedures to allow non-cleared individuals access to controlled offices
- ❑ **Develop** media marking, physical control, storage and disposal requirements for assigned sensitive information
- ❑ **Make sure** audit tools are used to track user activities on assigned system
- ❑ **Identify** and **limit** access to utilities, applications and scripts that bypass security controls
- ❑ **Control** access to remote / dial-up facilities and **protect** these facilities from unauthorized use

- ❑ **Make sure** procedures for issuing and managing passwords are followed
- ❑ **Advise and consent** on contractor recommendations for system procedures and changes that affect system security
- ❑ **Make sure** Disaster Recovery Plans exist. Disaster Recovery Plans specify steps to restore operations as a result of an incident that endangers the people and property of SFA or interrupts SFA operations
- ❑ **Review and recommend** changes to Disaster Recovery Plans
- ❑ **Determine** the need for encryption technologies where sensitive data transmissions occur

System Manager (SM)

- ❑ Make sure contractors **develop** a security plan for each assigned system. Make sure each plan is updated annually
- ❑ Make sure contractors **develop** Disaster Recovery, Contingency and Continuity of Operations Plans for each assigned system to make sure operations continue if the primary supporting infrastructure fails
- ❑ **Document** the various user positions and their related responsibilities and system privileges. Restrict each user's privileges to only those needed to accomplish their job.
- ❑ Make sure contractors **develop** control processes to review the operational and security impacts of proposed system changes. Processes should address approval,

testing and acceptance of changes prior to implementation

- ❑ **Create** procedures for users to request software. System and Network Administrators will review the requested software and determine if it can be provided to the user
- ❑ **Establish** workflow processes to protect the integrity of transactions as materials are passed from one person to another, particularly across organizational boundaries
- ❑ **Identify** system information exchanges and associated formats and protection
- ❑ **Establish** training requirements for users and managers of assigned systems
- ❑ **Establish** screening procedures for individual users assigned to a system
- ❑ **Restrict** system access to only those people necessary to perform their job
- ❑ **Designate** control areas for those areas supporting assigned system
- ❑ **Make sure** all system development efforts are accomplished exclusively in a development environment that reflects the operational environment, and tested with approved test data to reduce the risk of compromising data
- ❑ **Make sure** configuration and change management policies are followed when making system or system environment changes
- ❑ **Conduct** a system risk assessment at least every three years and develop a risk mitigation strategy

□ As designated Certifying Official, **Certify / Re-certify** each assigned system meets applicable SFA and Federal policies, regulations and standards. Re-certification is required at least every three years. The three certification options are:

- (1) Unconditional Certification,
- (2) Conditional Certification, or
- (3) Refuse Certification.

□ **Forward** system certification and accreditation package to DAA. Brief FM and SPA on certification findings and recommend accreditation outcome.

RESPONSIBILITIES OF SYSTEMS PERSONNEL



DESCRIPTION:

If the Security Management team answers the *what* and *why* of security, **Systems** personnel answer the *how*. You help drive the daily operation and maintenance of SFA systems, telecommunications networks, and information technology equipment in the capacity of:

- System Managers,
- Network Managers,
- System Administrators,
- Network Administrators,
- Database Administrators, and
- System Developers and Programmers.

You help design and develop the technical controls to implement SFA security and privacy policies. Once solutions are designed and implemented, you help monitor the effectiveness of the controls and recommend improvements.

The four types of security apply to systems personnel as they do in the other areas.

Administrative Security supports the safe operation of information systems. You should be aware of the

specific administrative activities that sustain SFA security, to include issuing and maintaining passwords, developing detailed contingency, continuity of operations and disaster recovery procedures, setting up user-associated system permissions, and following configuration and change management procedures.

You also interact significantly with **Personnel Security** by providing access to end-users. Personnel Security provides the background checks and clearances necessary to allow system access.

Successful personnel security requires positively identifying individuals accessing specific information. The key is creating and maintaining user accounts that match system privileges with job needs. Promptly processing authorized requests for the creation of system accounts will help minimize the possibility of users sharing system access. Additionally, you should review requested system access to correlate user duties and responsibilities to requested privileges for your system. Lastly, as directed by the SSO, you should restrict or revoke privileges of those who violate the intent of any security policies.

Systems practitioners also play a significant role in securing the physical assets of SFA. **Physical Security** emphasizes safeguarding SFA locations, employees, physical assets, and sensitive information. Securing the physical resources of SFA requires Systems practitioners to place physical assets in safe locations, to route communication networks in a secure manner, to develop and test Disaster Recovery Plans, to maintain asset inventories, and to develop procedures for storing and transferring assets. Close coordination between the Systems practitioners and the Security Management team is necessary to make sure that all assets are

identified, asset values are assigned, and protection / recovery plans meet SFA needs.



Most of the Systems security effort focuses on the area of **Information Security**, which includes designing, developing and implementing technical security controls. These controls can be developing application software to execute specific policy activities, maintaining user and access control lists, configuring hardware and software, or many others. Some specific examples are:

- Identifying, authenticating and authorizing system users;
- Allocating system resources based on assigned user privileges;
- Implementing and analyzing system audit logs to track and record user activities;
- Implementing controls to prevent users, whether intentionally or unintentionally, from altering their assigned privileges, or bypassing installed security features;
- Implementing separate security applications and hardware to protect systems, networks, and transactions from malicious activities and unauthorized disclosure;
- Following configuration management policies and

procedures as identified by system security plans and SFA guidance

- Discussing security and privacy standards with the SM, SSO and CSO as requirements arise or change.



THINGS TO DO:

System Security Officer (SSO)

- **Limit** and **control** access to Departmental networks to authorized users only
- **Consider** disaster recovery procedures prior to physical routing of network cable and the physical location of network support equipment
- **Review** user accounts to validate access privileges and pass any required account changes to system administrator
- **Monitor** the security status of the assigned network and report anomalies to SM, SPA, and CSO
- **Develop** necessary security controls to operate the LAN / WAN

System Manager (SM)

- **Document** expected system event procedures, such as system start-up and initialization, system shut-down, database updates, and software changes
- **Document** abnormal events, such as system failures, unsuccessful system initializations or shut-downs, system error responses, and corruption or loss of data
- **Authorize** system access only after confirming personnel have appropriate clearance and need

- ❑ **Maintain** and **secure** all system software, data, and documentation at an off-site location to support the Disaster Recovery Plan, the Contingency Plan, and the Continuity of Operations Plan.
- ❑ **Approve** requests for services that are necessary and properly documented

System Administrator

- ❑ **Make sure** password procedures for assigned systems meet SFA and Department of Education standards
- ❑ **Make sure** personnel security clearances are complete and properly documented prior to issuing system access / password
- ❑ **Make sure** permissions granted are specific to the individual position and system role / responsibility
- ❑ **Make sure** written system procedures are accurate and recommend changes to the SM
- ❑ **Make sure** all system administration materials required to support the Disaster Recovery, Contingency and Continuity of Operations Plans are pre-staged at the designated safe location
- ❑ **Identify** authorized users through the use of unique user IDs and passwords
- ❑ **Implement** terminal screen lock-outs after a pre-determined time of inactivity to prevent access to non-authorized users
- ❑ **Isolate** users from operating system configurations and command prompts

- ❑ **Make sure** system errors do not allow users to system execution permissions, nor allow users to access command prompts, or attain additional privileges
- ❑ **Implement** system logs and controls to allow for identifying, recording, reporting, and assigning accountability for activities that occur within an information system
- ❑ **Restrict** access to system utilities that may bypass or execute security controls
- ❑ **Restrict** users' ability to install any software
- ❑ **Revoke** access to invalid users
- ❑ **Prohibit** development personnel from moving material from the test environment to the production environment

Network Administrator

- ❑ **Make sure** password procedures for assigned systems meet SFA and Department of Education standards
- ❑ **Review** Disaster Recovery, Contingency and Continuity of Operations Plans. Recommend changes to the System Manager and SSO
- ❑ **Make sure** personnel security clearances are complete and properly documented before forwarding to System Administrator
- ❑ **Make sure** all network administration materials required to support the Disaster Recovery, Contingency and Continuity of Operations Plans are pre-staged at the designated safe location

- ❑ **Install** and **monitor** the operation of protective software (e.g. virus protection, intrusion detection) in accordance with policy and direction from SM and FM
- ❑ **Make sure** installed network encryption services operate properly and effectively
- ❑ **Authenticate** transactions with other organizations
- ❑ **Distribute** remote access numbers only to authorized users
- ❑ **Implement** remote access controls
- ❑ **Close** communications ports when the communication path is terminated normally or abnormally
- ❑ **Assume** network services remain unavailable unless specifically necessary and approved for operation

Database Administrator

- ❑ **Review** Disaster Recovery, Contingency and Continuity of Operations Plans and recommend changes to the SM and SSO
- ❑ **Review** written system procedures for accuracy and recommend changes to SM
- ❑ **Make sure** all database administration materials required to support the Disaster Recovery, Contingency and Continuity of Operations Plans are pre-staged at the designated safe location
- ❑ **Implement** database logs to associate data changes with specific users
- ❑ **Enforce** the use of database access methods, which incorporate data integrity checks

- ❑ **Limit** direct database access to database administrators

System Developer

- ❑ **Make sure** system documentation is updated to maintain currency with system changes
- ❑ **Trap** system malfunctions and user errors to guide the user to a controlled exit of the interface, and if necessary, the application
- ❑ **Implement** transaction assurance procedures, such as error detection and checksum comparisons, for data transfers between system resources
- ❑ **Test** newly developed software prior to moving into the production environment
- ❑ **Prohibit** developers from directly accessing production libraries, except where authorization is granted by the SM and SSO
- ❑ **Develop** test data for system testing, making sure operational data is not used during system testing
- ❑ **Notify** the network administrator of necessary network services that must be approved by the system manager

ACQUISITION RESPONSIBILITIES



DESCRIPTION:

If you are involved with the acquisition of IT products or services, then this section provides guidance specific to your role in SFA. Some of you will be involved in establishing contracts and programming money. Others will be developing system requirements and operational constraints. Some acquisition personnel will be responsible for supervising the delivery of services or materials. Because the acquisition process interacts with the entire system lifecycle, you must thoroughly understand each procurement's goals and objectives. These must fully support the successful, secure realization of SFA's goals.

The acquisition process is not just a "see it - buy it" activity. It requires involvement from the moment an idea is conceived to the design, implementation, and retirement of the system. Fortunately, the daily fulfillment of your job will help you assess security shortfalls throughout the System Life Cycle.

Awareness of the security requirements in the acquisition process can increase your understanding of each system's current state and your specific security responsibilities.



THINGS TO DO:

Functional Manager

- ❑ **Review** future development efforts with the CSO, SPA, SM, and SSO to make sure that security is handled in a consistent manner across the department, and that it complies with federal oversight requirements
- ❑ **Review** design specification risk analyses before approving any new system or major system modification
- ❑ **Make sure** the prospective offeror meets the security requirements of the solicitation prior to the award for acquisition of new systems or technology resources

(The Functional Manager can support this review through the appointment of any Department employee to conduct the security requirement review of the offeror. The Functional Manager can recommend certification based on the review. If the review indicates non-compliance with department security policy, the Functional Manager must advise the Contracting Officer of the non-compliance.)

Contracting Officer's Technical Representative (COTR)

- ❑ **Require** offeror to present a detailed outline of proposed information technology security program and document compliance with the SFA security requirements
- ❑ **Make sure** technical proposal instructions include a statement of security compliance requiring the offeror to comply with the security requirements identified in the

statement of work (*This clause must include 'flow-down coverage' to make sure all sub-contractors used to support the work effort will also meet the requirements identified in the clause.*)

- ❑ **Provide** applicable SFA security documents upon request
- ❑ **Inform** offerors about the Contractor Self Certification Program for Low-Risk ADP related responsibilities for low risk efforts

Computer Security Officer (CSO)

- ❑ **Review** the contract for compliance with SFA security policy. Assist the Functional Manager and the Contracting Officer with these efforts
- ❑ **Help Develop** standard contract language and / or performance standards for SFA contracts

System Security Officer (SSO)

- ❑ **Support** the Functional Manager in identifying and developing security requirements for new systems and system enhancements

SECTION II GUIDE TO SECURITY OF FEDERAL AUTOMATED INFORMATION RESOURCES

INFORMATION SECURITY IS VITAL TO SFA SUCCESS

The previous section provided guidance for the role each SFA employee might play in information security. While still applicable to all employees, this section provides some of the specifics contributing to the overall management of SFA information systems. The government has taken serious initiatives to protect information, some of which are documented in OMB Circular A-130. The following are excerpts, which provides authoritative guidance on implementing the Computer Security Act:

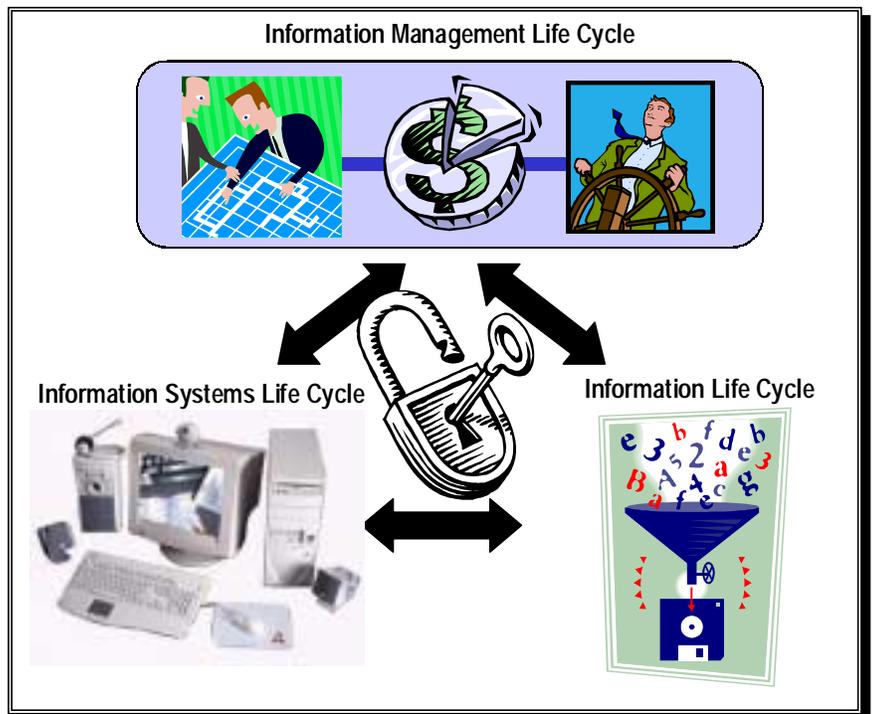
The Federal Government is the largest single producer, collector, consumer, and disseminator of information in the United States....

...(T)he public disclosure of government information is essential to the operation of a democracy....

The individual's right to privacy must be protected in Federal Government information activities....

We protect customers' privacy and data by managing the following life cycles:

- Information Management Life Cycle - **Planning, budgeting, manipulating** and **controlling** information.
- Information Systems Life Cycle - The phases through which an information system passes, typically characterized as **initiation, development, operation,** and **termination.**
- Information Life Cycle - The stages through which information passes, such as **creation or collection, processing, dissemination, use, storage,** and **disposition.**

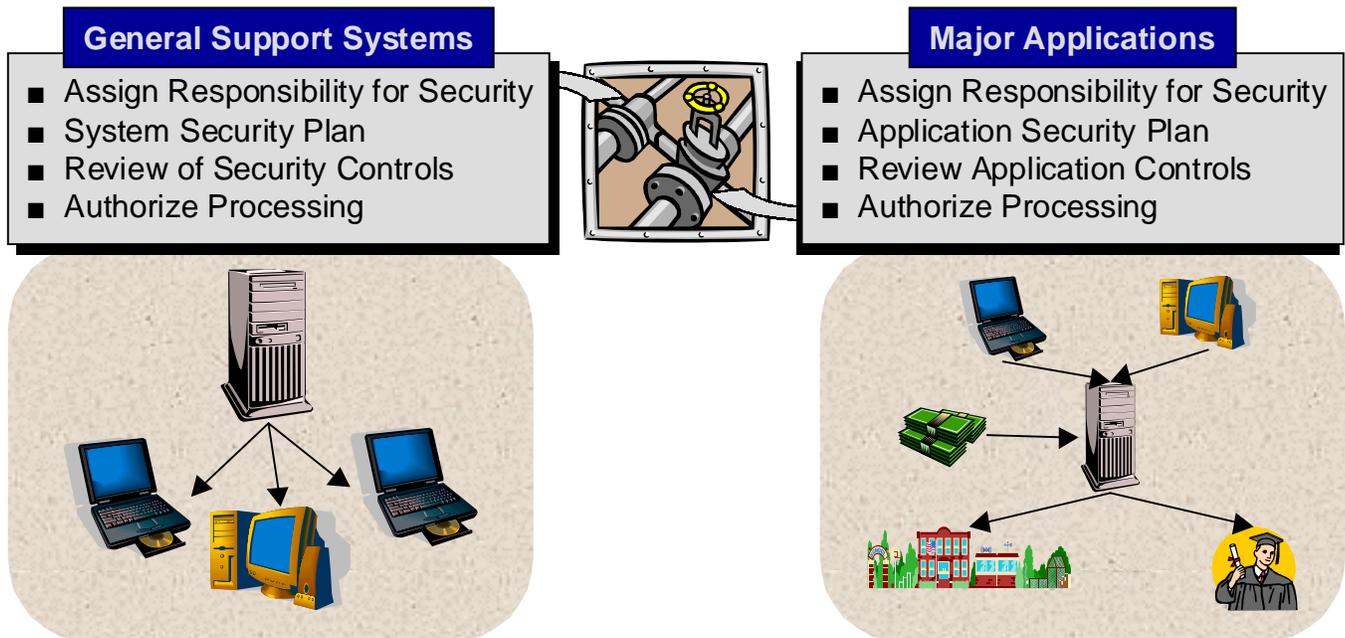


PUTTING SECURITY TO WORK IN THE LIFE CYCLE

Incorporating security and privacy protection into all these life cycle activities can seem overwhelming. Consequently, our friends at OMB focused on two sets of support systems:

- General Support Systems - Interconnected set of information resources under the same direct management. For example, the Title IV Wide Area network (TIV WAN), which is a sensitive general support system providing services to most SFA applications. It contains Privacy Act data, stores and transmits information that can be used to access other sensitive applications, processes financial data (cost-recovery and billing information), and contains components of significant value to the Government.
- Major Applications - Information and technology that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to the information in the application, i.e., Central Processing System (CPS), which provides a centralized system for processing student aid application and determining eligibility for aid.

Each of these systems has a set of controls, which govern how security will be implemented. As depicted below, you can see that similar activities occur between both General Support Systems and Major Applications.

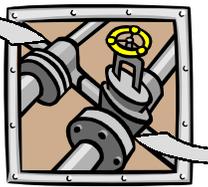


The next few pages will explain the bullets and provide a guide for you to follow as you assemble a security system around either your General Support Systems or Major Applications. Where possible, explanations occur on both sides of the diagram to demonstrate the similarities and differences between the "Systems" and "Applications".

SECURITY OF FEDERAL AUTOMATED INFORMATION RESOURCES

General Support Systems

- **Assign Responsibility for Security**
 - System Security Plan
 - Review of Security Controls
 - Authorize Processing

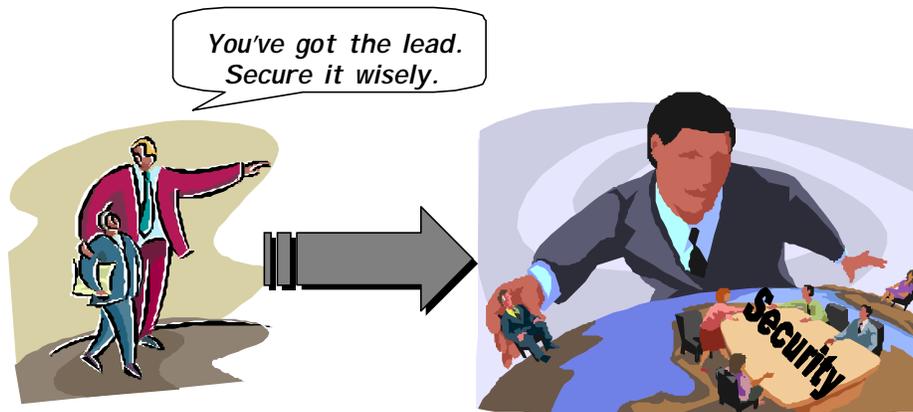


Major Applications

- **Assign Responsibility for Security**
 - Application Security Plan
 - Review Application Controls
 - Authorize Processing

- **Individual should know about:**
 - Information technology used in the system
 - Providing security for such technology

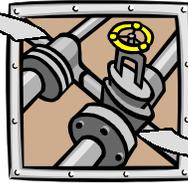
- **A manager who knows about:**
 - Nature of the information
 - Process supported by the application
 - Management, personnel, operational, and technical controls used to protect it
- **A manager should make sure effective security products and techniques are used**
- **A manager serves as the primary point of contact when a security incident occurs**



SECURITY OF FEDERAL AUTOMATED INFORMATION RESOURCES

General Support Systems

- Assign Responsibility for Security
- **System Security Plan**
- Review of Security Controls
- Authorize Processing



Major Applications

- Assign Responsibility for Security
- **Application Security Plan**
- Review Application Controls
- Authorize Processing

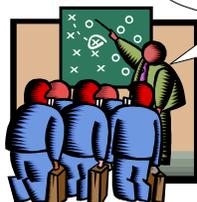
- **Rules of the System**
- Training
- Personnel Controls
- Incident Response Capability
- Continuity of Support
- Technical Security
- System Interconnection

- **Application Rules**
- Specialized Training
- Personnel Security
- Contingency Planning
- Technical Controls
- Information Sharing
- Public Access Controls

- **Consider the various users of the systems and determine necessary level of security and risk**
- **Assign responsibilities and outline expected behavior from all system users**
- **Set limits on interconnections with other systems**
- **Outline consequences if rules not followed**

- **Establish rules concerning use of and behavior within the application**
- **Clearly define responsibilities and expected behavior of individuals with access to application**
- **Set limits on interconnections with other systems**
- **Outline ramifications if rules not followed**

- ✓ Do you have high risk systems coupled with low risk people?
- ✓ Did you clearly outline the "Dos" and "Don'ts" of system use?
- ✓ Does everyone know with what they can interconnect?
- ✓ Does everyone know what will happen if they violate the rules?



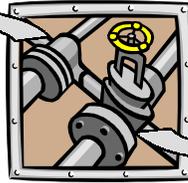
SECURITY OF FEDERAL AUTOMATED INFORMATION RESOURCES

General Support Systems

Major Applications

- Assign Responsibility for Security
- **System Security Plan**
- Review of Security Controls
- Authorize Processing

- Assign Responsibility for Security
- **Application Security Plan**
- Review Application Controls
- Authorize Processing



- Rules of the System
- **Training**
- Personnel Controls
- Incident Response Capability
- Continuity of Support
- Technical Security
- System Interconnection

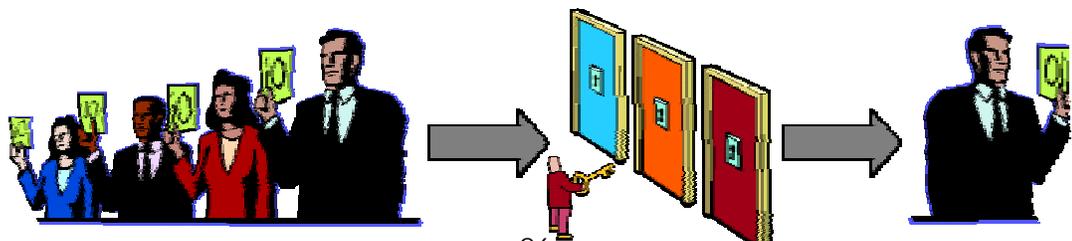
- Application Rules
- **Specialized Training**
- Personnel Security
- Contingency Planning
- Technical Controls
- Information Sharing
- Public Access Controls

- **Train all personnel in how to fulfill their security responsibilities before system access**
- **Inform personnel of available assistance and technical security products and techniques**
- **Provide refresher training**

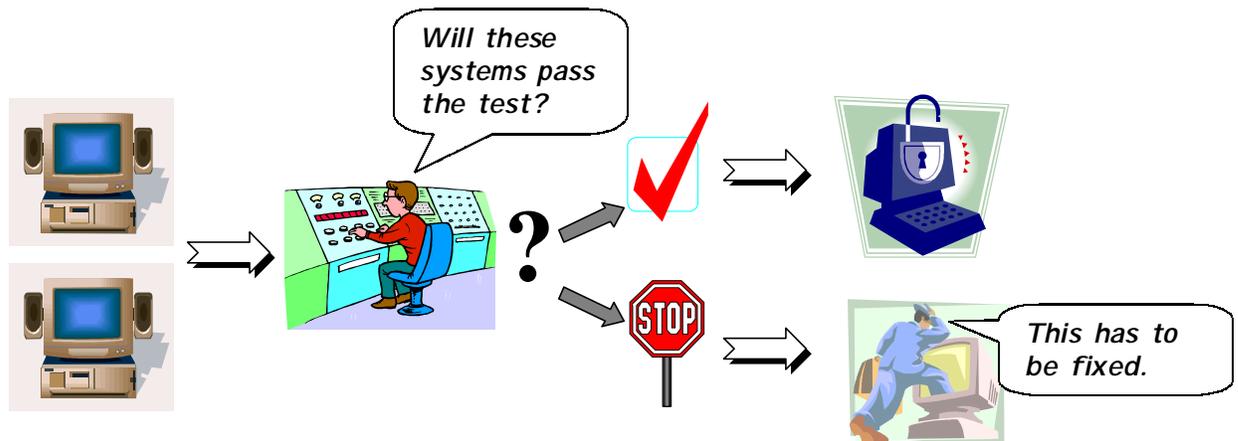
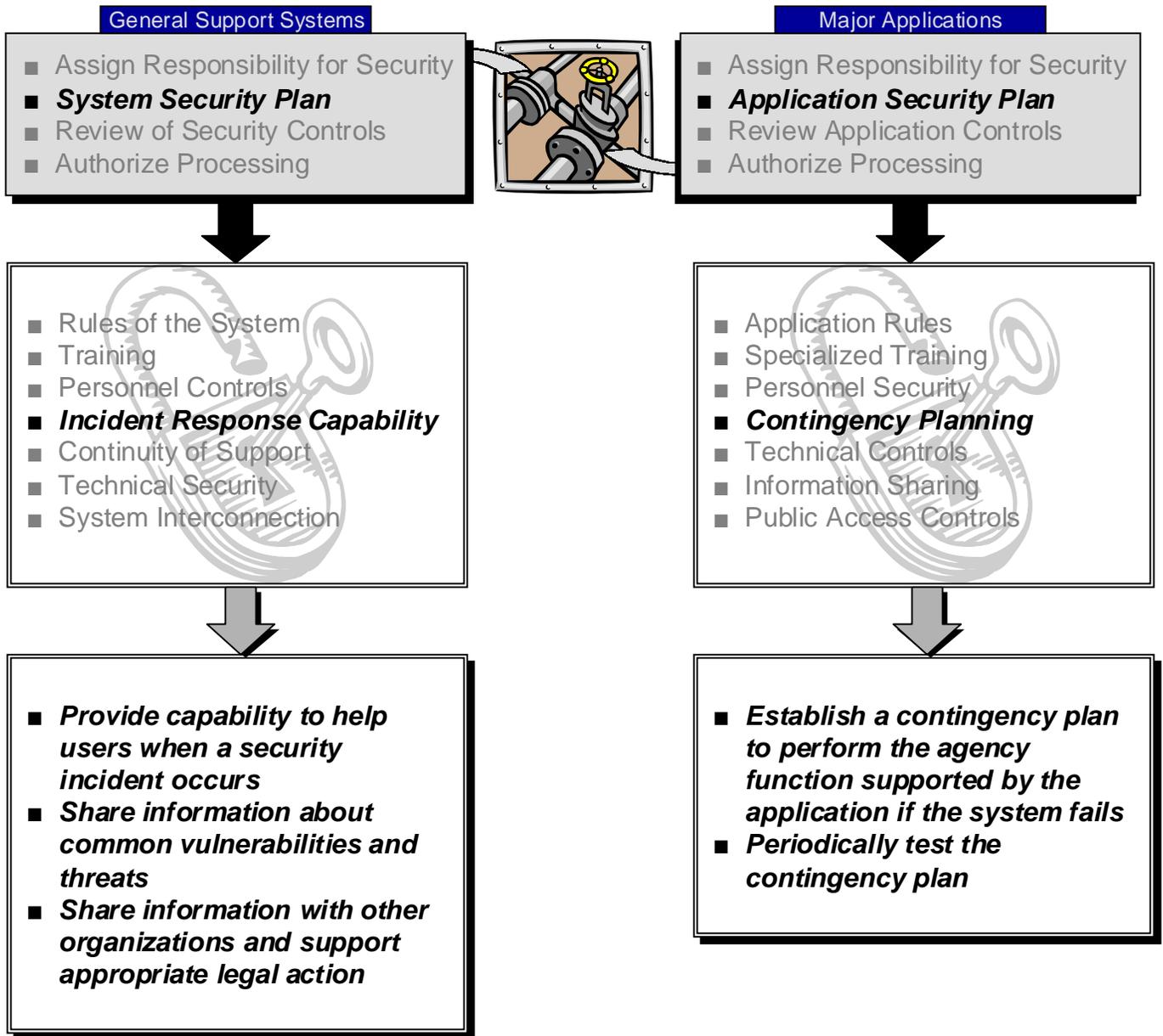
- **Provide specialized training to all individuals, which focuses on their specific responsibilities and application rules, in addition to the General Systems training they receive**



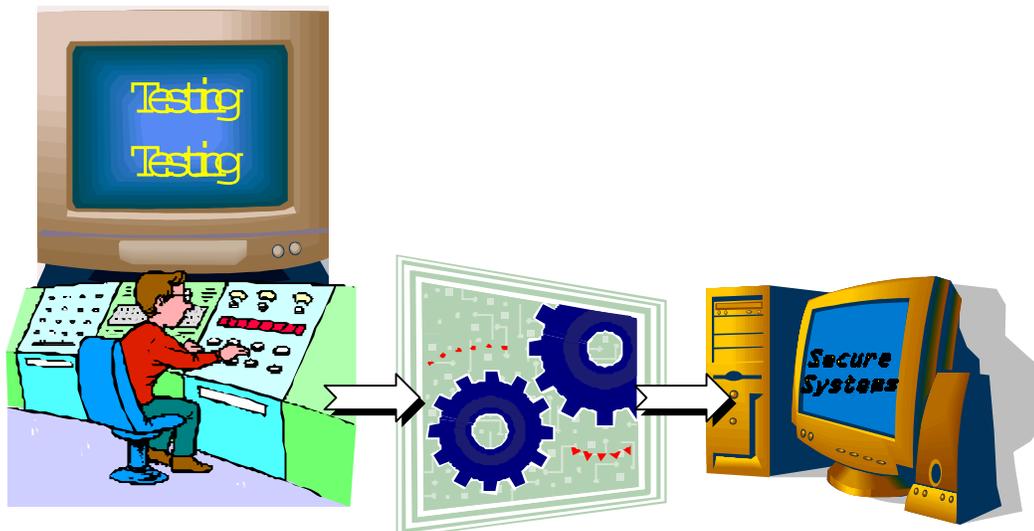
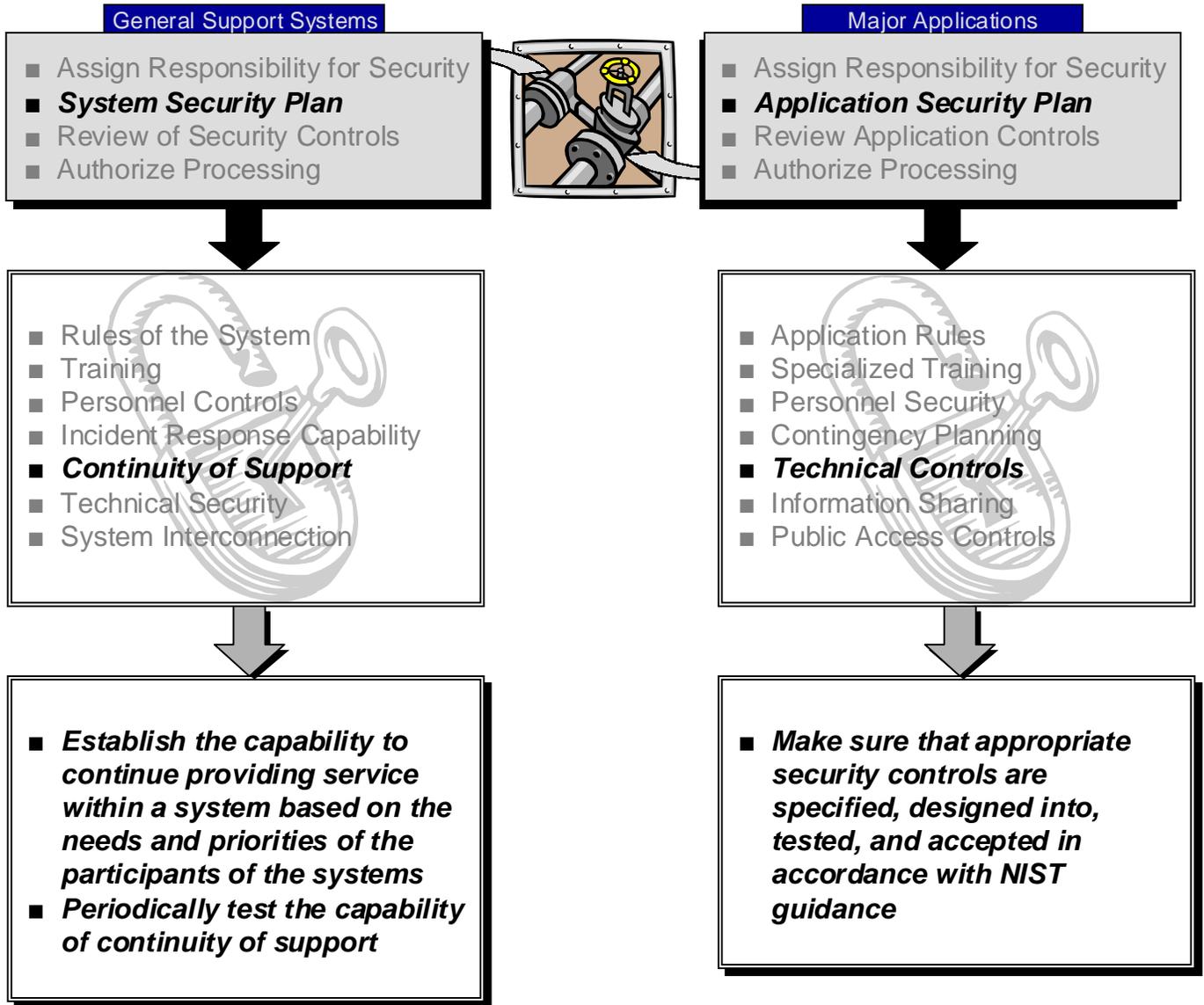
SECURITY OF FEDERAL AUTOMATED INFORMATION RESOURCES



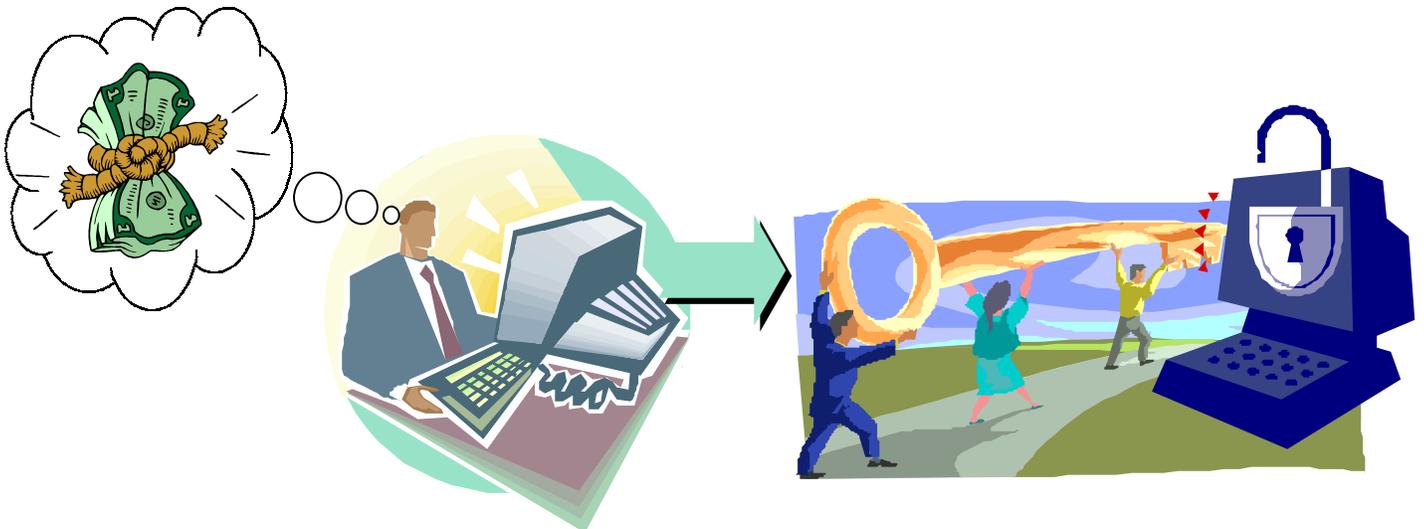
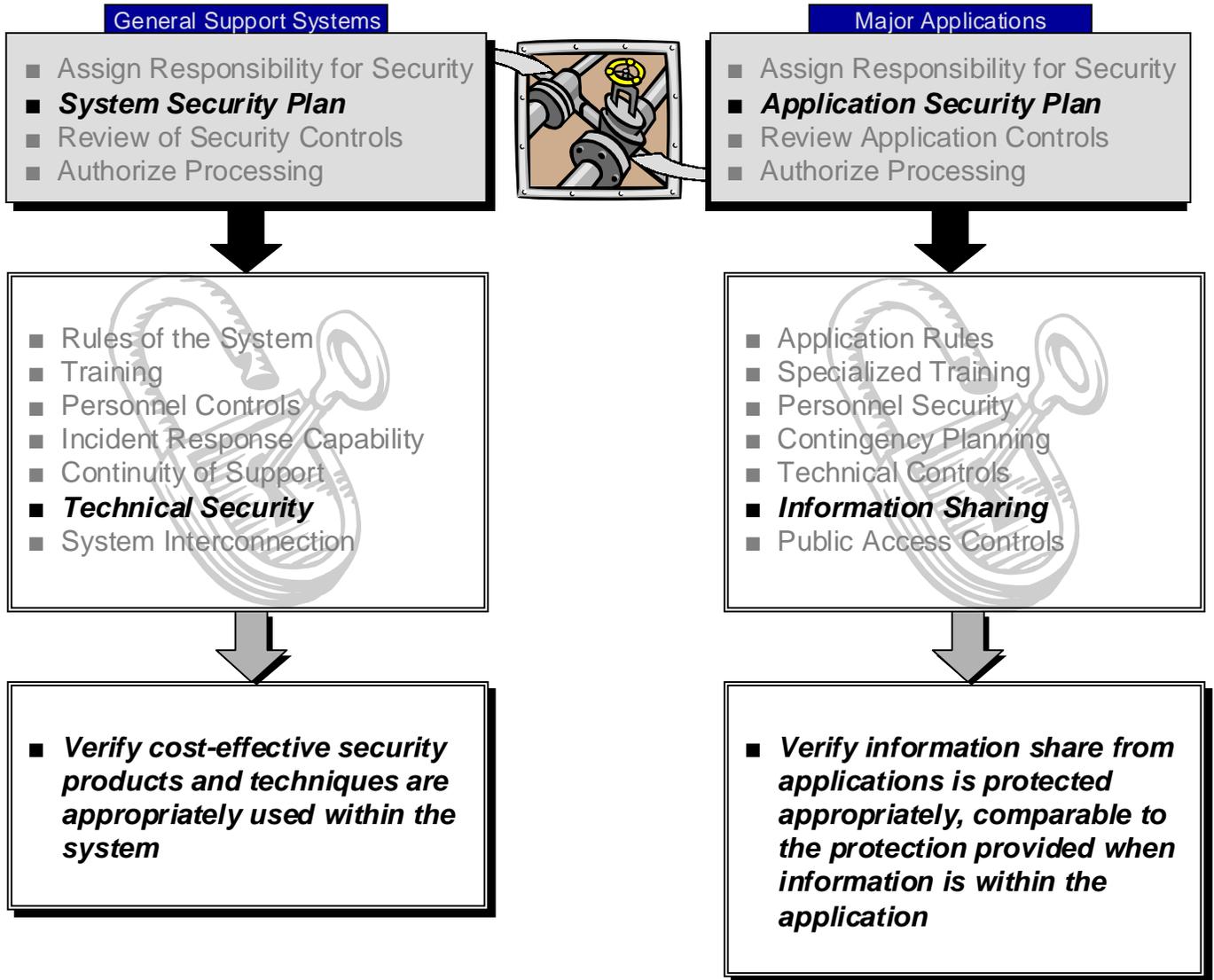
SECURITY OF FEDERAL AUTOMATED INFORMATION RESOURCES



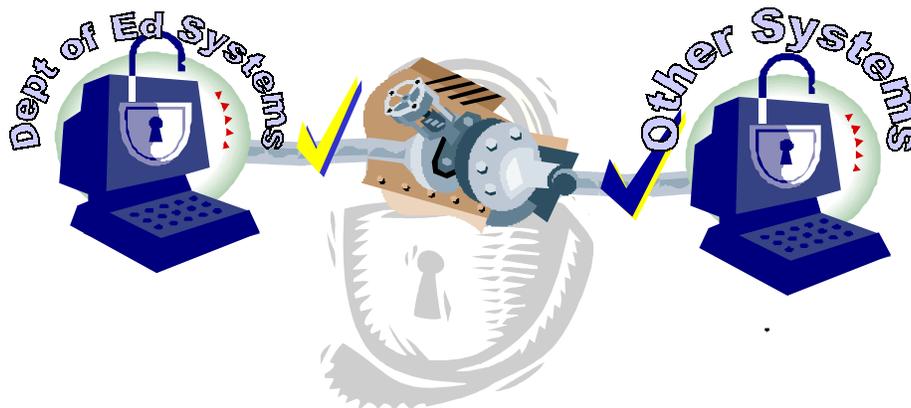
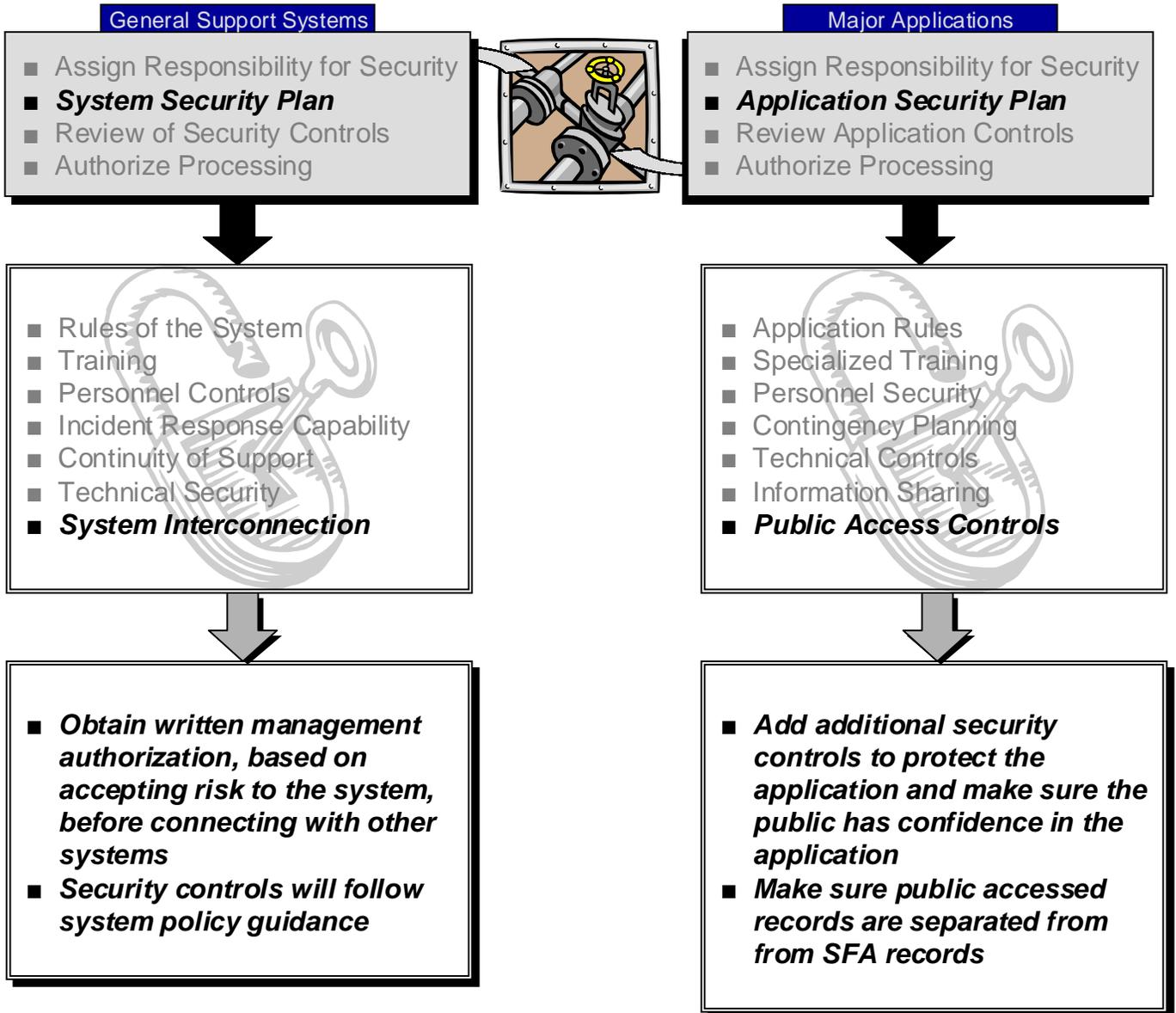
SECURITY OF FEDERAL AUTOMATED INFORMATION RESOURCES



SECURITY OF FEDERAL AUTOMATED INFORMATION RESOURCES



SECURITY OF FEDERAL AUTOMATED INFORMATION RESOURCES



SECURITY OF FEDERAL AUTOMATED INFORMATION RESOURCES

General Support Systems

- Assign Responsibility for Security
- System Security Plan
- **Review of Security Controls**
- Authorize Processing

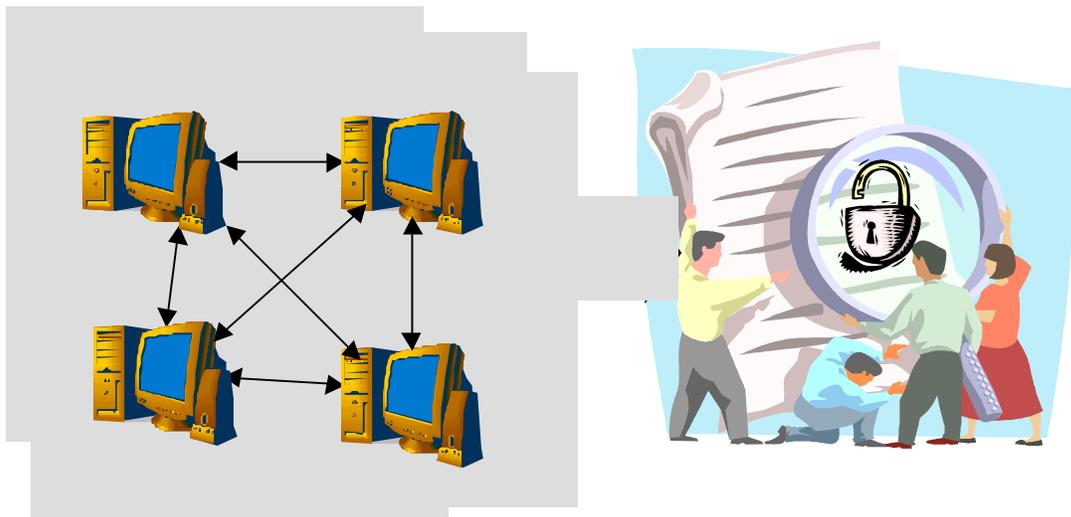


Major Applications

- Assign Responsibility for Security
- Application Security Plan
- **Review Application Controls**
- Authorize Processing

- **Review security controls when significant modifications are made to the system or every three years**
- **Determine the scope and frequency of the controls based on the acceptable level of risk for the system**
- **Identify deficiencies described in OMB Circular No A-123 if there is no assignment of the following:**
 - Security Responsibility
 - Security Plan
 - Authorization to Process

- **Perform independent review or audit of security controls at least every three years**
- **Identify deficiencies pursuant to OMB Circular No A-123 if there is no assignment of the following:**
 - Security Responsibility
 - Security Plan
 - Authorization to Process



SECURITY OF FEDERAL AUTOMATED INFORMATION RESOURCES

