



# The Authorizing Official (AO)

## DOE EM Role Based Training





The reason  
why your role  
is critical...

## Department of Energy hit by 'sophisticated' cyber-attack - and authorities believe Chinese hackers could be behind it

- U.S. Department of Energy was hacked in 'sophisticated' attack two weeks ago, Washington-based paper reports
- Thousands of personal files stolen, and authorities believe hackers could have been after classified documents
- Comes on the heels of New York Times, Wall Street Journal, and Washington Post hackings

By BETH STEBNER

PUBLISHED: 13:01 EST, 4 February 2013 | UPDATED: 16:03 EST, 4 February 2013



0 View comments

The U.S. Department of Energy suffered a major security breach after a large cyber-attack that targeted computer networks, it was revealed today.

The [Washington Free Beacon](#) reported that an unknown group targeted the government organization two weeks ago and harvested the personal information of several hundred of its employees.

While the agency says that no confidential data was compromised, experts said that attackers could have been targeting that data.

**Scroll down for letter to government employees**





# Key Goals of Cyber Security

- Ensuring that all computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction
- protection from unauthorized activities or untrustworthy individuals, but also from unplanned events and natural disasters
- managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data



# Objectives

Gain Understanding and Working Knowledge of:

- AO Authority, Role and Responsibilities
- AO Structure
- Key Cyber Security Terms
- Cyber Security Program Management Structure
- Policy Hierarchy
- Risk Management Framework and Certification & Accreditation Process Relationship
- Accreditation Forms, Boundaries, Common Controls and Inheritance
- AO C&A Package Review
- Accreditation Decision
- Continuous Monitoring





# Who is the AO?

## DOE Authorizing Authority (AO)

- Responsible for Protection of Information and Information Technology for the DOE
- Responsible for Oversight of EM Field Site Cyber Security Program which includes
  - DOE EM Organizations
  - Contractors
  - Sub-contractors
- Fully accountable for information system operation at an acceptable level of risk





# What does the AO do?

## Authorizing Official (AO)

- Ensures that the requirements of the RMAIP are implemented.
- Accepts risk for the operation of an IT system.
- Directly appoints, in writing, a federal employee as the AO Designated Representative (AODR).
- Furnishes a copy of the appointment letter for the AODR to the Cyber Security Program Manager at EM Headquarters as well as the site Information System Security Manager (ISSM) within 60 days of appointment.
- Appoints a new or Acting AODR in the event of personnel turnover or extended absence of the AODR. An appointment letter for a new or Acting AODR shall be disseminated within twenty one (21) business days of the departure of the previous AODR.
- Ensures direct access to the AODR for all cyber security matters.
- Receives, at least quarterly, a formal cyber security status briefing directly from the AODR.
- Ensures that personnel are appointed, in writing, to the roles of System Owner, ISSM, Information System Security Officer (ISSO), and Information Technology Contingency Planning Director.

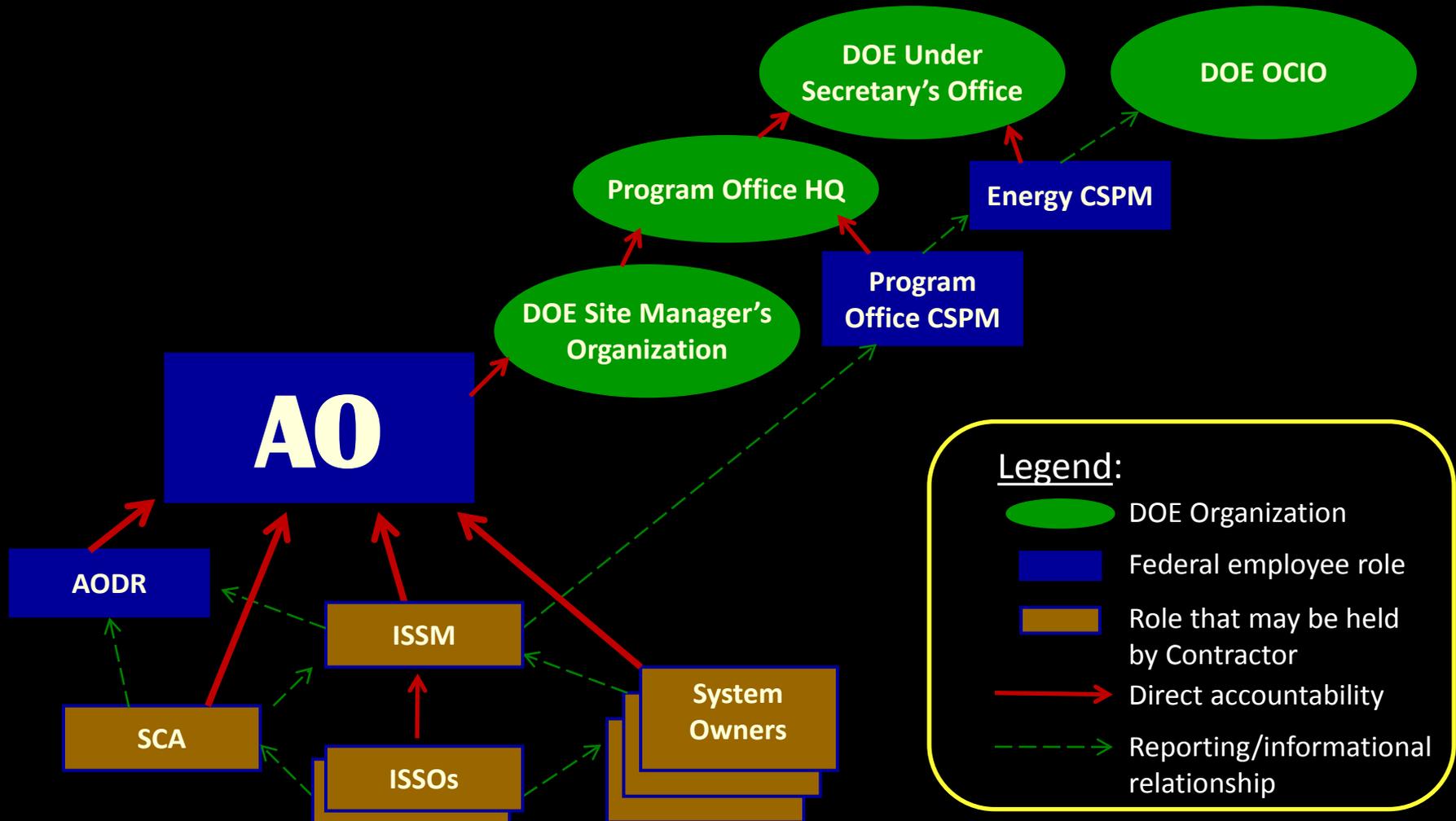


## To Summarize...

The **Authorizing Official** is a federal **senior management official** with budget and oversight authorities within the organization who **assumes the responsibility** for an information system and is **held accountable** for ensuring the information system is operating at an acceptable level of risk.



# AO Accountability Structure





# EM Cyber Security Management Structure

## DOE Cyber Security Management Structure Key Roles

- **Cyber Security Program Manager(CSPM)**
- **AO Designated Representative(AODR)**
- **Information Systems Security Manager(ISSM)**
- **Certification Agent(CA) or Security Control Assessor**
- **System Owner**
- **Information System Security Officer (ISSO)**



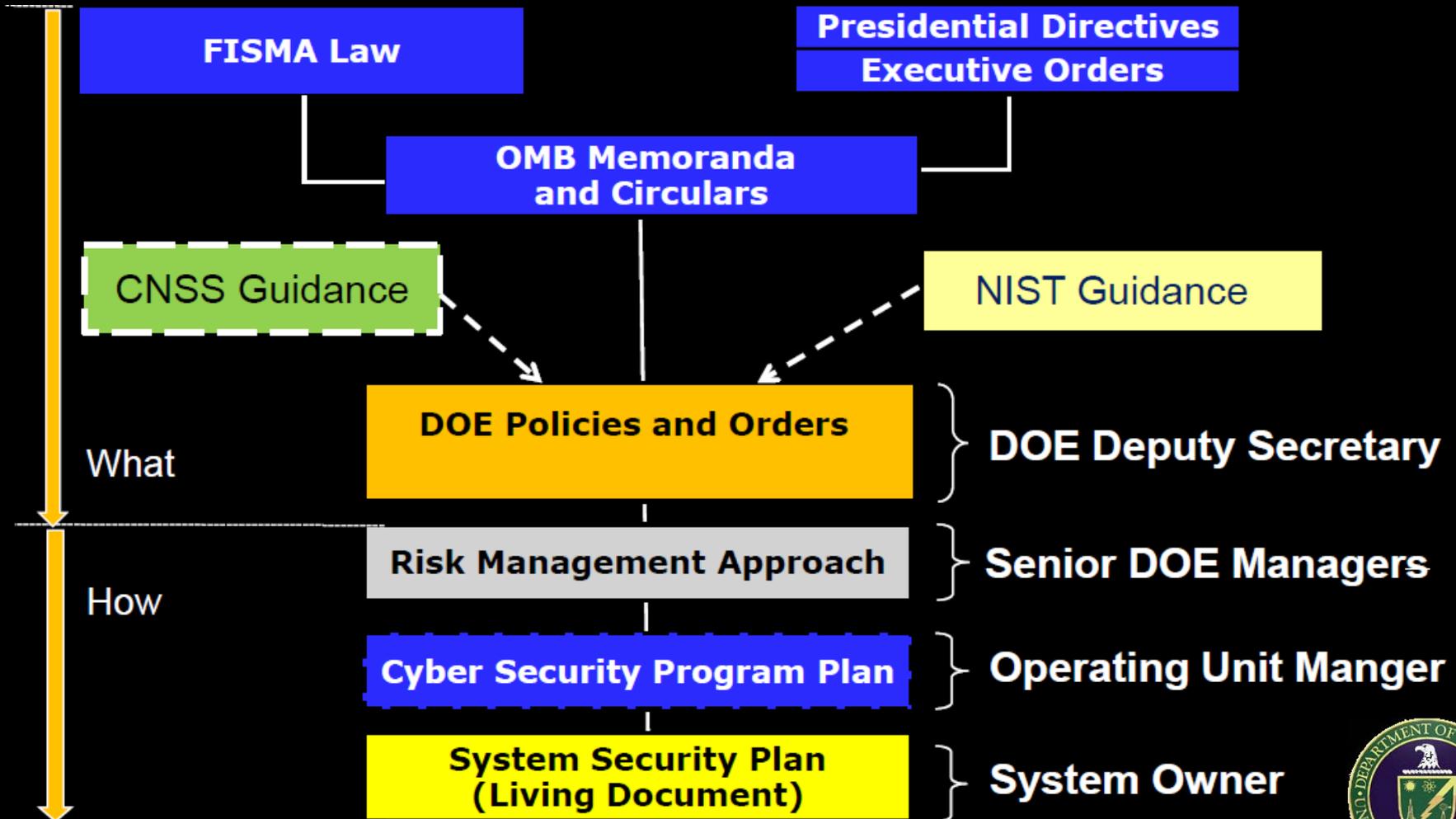


# Laws, Policies, Orders & Guidance





# The Policy Hierarchy





# The Policy Hierarchy

## Office of the Chief Information Officer *The Policy Hierarchy*

- **DOE O 205.1B and the RMAIP establish a DOE Cyber Security Program**
  - Requires the Senior DOE Managers to Implement a Cyber Security Program
  - Develop a Risk Management Approach (RMA)
- **DOE Cyber Security Policy and Orders are based on requirements and guidance from**
  - Office of Management and Budget
  - National Institute of Standards and Technology
  - Committee for National Security Systems Instructions





# Law - FISMA

- **FISMA**

“Each federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source...”

-- Federal Information Security Management Act of 2002

## H. R. 2458—48

- (1) maximize the degree to which unclassified geographic information from various sources can be made electronically compatible and accessible; and
- (2) promote the development of interoperable geographic information systems technologies that shall—
  - (A) allow widespread, low-cost use and sharing of geographic data by Federal agencies, State, local, and tribal governments, and the public; and
  - (B) enable the enhancement of services using geographic data.
- (f) **AUTHORIZATION OF APPROPRIATIONS.**—There are authorized to be appropriated such sums as are necessary to carry out this section, for each of the fiscal years 2003 through 2007.

### **TITLE III—INFORMATION SECURITY**

#### **SEC. 301. INFORMATION SECURITY.**

(a) **SHORT TITLE.**—This title may be cited as the “Federal

Information Security Management Act of 2002”.

(b) **INFORMATION SECURITY.**—

(1) **IN GENERAL.**—Chapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter:

“**SUBCHAPTER III—INFORMATION SECURITY**

“**§ 3541. Purposes**



# Key Provisions of the FISMA Law

## Department of Energy (DOE)



- Agencies must **inventory** their IT assets
- Agencies must **assess risk**
- Agencies must **implement protections** commensurate with the level of risk
- Agencies must **implement policies** to reduce the level of risk
- Agencies must **conduct testing** to ensure that controls are effectively implemented
- Agencies must **provide security awareness training**



## National Institute of Standards and Technology (NIST)

- NIST is empowered to **define** federal information security standards



# Order - DOE Order 205.1B

- Requires a Departmental Cyber Security Program (CSP) that protects information and information systems for the Department of Energy (DOE)
- A Risk Management Approach (RMA) that includes: analysis of threats/risks; risk-based decisions considering security, cost and mission effectiveness; and implementation
- Consistent with the National Institute of Standards and Technology (NIST) guidelines and the Committee on National Security Systems (CNSS) cyber requirements, processes and protections
- Emphasizes risk management rather than a systems-level “controls compliance” approach
- DOE Oversight is conducted through *Assurance Systems* that monitor the risk evaluation and protection processes at each level in the organization

U.S. Department of Energy  
Washington, D.C.

ORDER

DOE O 205.1B

Approved: 5-16-2011

SUBJECT: DEPARTMENT OF ENERGY CYBER SECURITY PROGRAM

1. **PURPOSE** To set forth requirements and responsibilities for a Departmental Cyber Security Program (CSP) that protects information and information systems for the Department of Energy (DOE). The CSP requires a Risk Management Approach (RMA) that includes: analysis of threats/risks; risk-based decisions considering security, cost and mission effectiveness; and implementation consistent with guidelines from the National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) cyber requirements, processes and protections. *DOE Oversight* is conducted through *Assurance Systems* that monitor the risk evaluation and protection processes at each level in the organization. The DOE CSP emphasizes risk management rather than a systems-level “controls compliance” approach. Through the RMA, the Department effectively and efficiently meets its obligations under the Federal Information Security Management Act (FISMA) in a manner that improves, rather than impedes the fulfillment of the Department’s statutory missions.

The CSP, through DOE’s RMA:

- a. establishes line management accountability for ensuring protection of information and information systems through Senior DOE Management (SDM) consisting of the Department’s Under Secretaries, the Energy Information Administrator, Power Marketing Administrators and the Chief Information Officer (CIO) (see *Attachment 3* for a pictorial representation of DOE SDM);
- b. recognizes the Department’s federated government-owned/contractor operated (GOCO) environment and appropriately integrates cyber security governance, accountability and reporting into management and work practices at all levels of the Department;
- c. institutes a mission-centric, risk-based approach to the management of cyber security to ensure the confidentiality, integrity, and availability of DOE information and information systems;
- d. requires a training, education, and awareness program that develops and maintains cyber security competencies including threat identification and risk management throughout DOE Federal and contractor workforces that enables personnel to fulfill their responsibilities in protecting DOE information and information systems;
- e. establishes cyber security governance processes that are mission-focused;
- f. defines enterprise-level cyber security requirements, processes and responsibilities for protecting unclassified and national security information and information systems; and

AVAILABLE ONLINE AT:  
[www.directives.doe.gov](http://www.directives.doe.gov)

INITIATED BY:  
Office of the Chief Information Officer



# Policy - RMAIP

- **Recognizes that the EM mission and business processes are dependent on the sites information technology (IT) infrastructure for the completion of the DOE mission**
- **Recognizes that Government systems are now being subjected to almost daily sophisticated security attacks where signature based protection programs, annual assessments and three-year static certification and accreditation processes are no longer effective.**
- **All EM systems are to be protected in a manner commensurate with the impact to EM's mission, acceptable risk levels, security requirements and potential magnitude of harm**
- **Implementation of Order 205.1B  
Supersedes older policies for EM (PCSP and PSP)**

---

**Office of Environmental Management (EM)  
Cyber Security Policy and  
Risk Management Approach Implementation  
Plan  
February 2014**

---



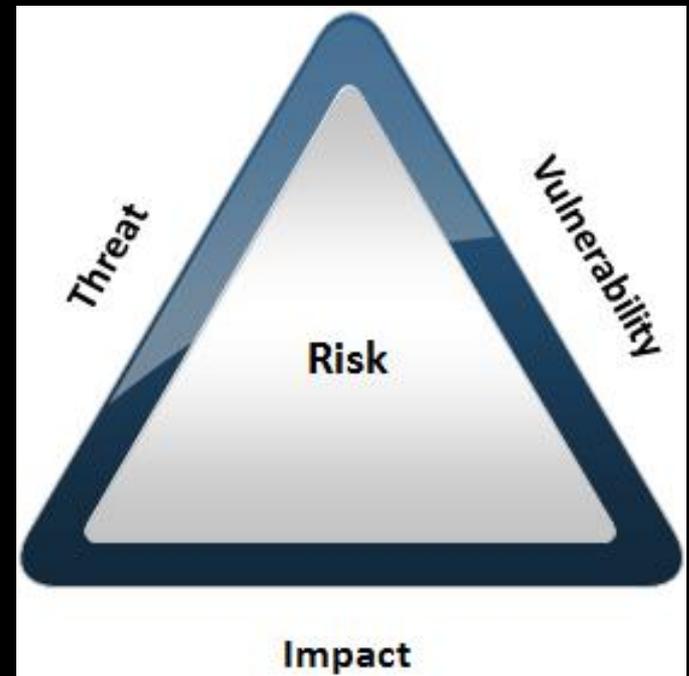
Office of Environmental Management  
U.S. Department of Energy  
Washington, DC

---



# Emphasis on Risk Management

- **Introduction of the Risk Management Approach (RMA)**
- **Four step process used in the assessment of risk during the continuous monitoring phase of the Risk Management Framework (RMF)**
- **RMA deals mainly with the identification, monitoring and management of risk based on mission needs**



# Policy Flow



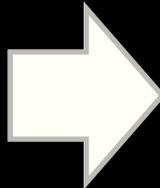
## FISMA H. R. 2458—48

- (1) maximize the degree to which unclassified geographic information from various sources can be made electronically compatible and accessible; and
- (2) promote the development of interoperable geographic information systems technologies that shall—
  - (A) allow widespread, low-cost use and sharing of geographic data by Federal agencies, State, local, and tribal governments, and the public; and
  - (B) enable the enhancement of services using geographic data.
- (f) **AUTHORIZATION OF APPROPRIATIONS.**—There are authorized to be appropriated such sums as are necessary to carry out this section, for each of the fiscal years 2003 through 2007.

### TITLE III—INFORMATION SECURITY

#### SEC. 301. INFORMATION SECURITY.

- (a) **SHORT TITLE.**—This title may be cited as the ‘‘Federal Information Security Management Act of 2002’’.
  - (b) **INFORMATION SECURITY.**—
    - (1) **IN GENERAL.**—Chapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter:  
‘‘SUBCHAPTER III—INFORMATION SECURITY  
‘‘§ 3541. Purposes



U.S. Department of Energy  
Washington, D.C.

ORDER  
DOE O 264-13  
Approval: 7-16-2013

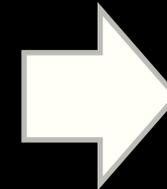
SUBJECT: DEPARTMENT OF ENERGY CYBER SECURITY PROGRAM

1. **PURPOSE.** To set forth requirements and responsibilities for a Departmental Cyber Security Program (CSP) that protects information and information systems for the Department of Energy (DOE). The CSP requires a Risk Management Approach (RMA) that includes: analysis of threat risks, risk-based decision computing security, cost and resource effectiveness, and implementation consistent with guidance from the National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) cyber requirements, practices and processes. DOE oversight is conducted through *discovery-driven* that require the risk evaluation and protection processes at each level in that organization. The DOE CSP emphasizes risk management rather than a systems-level ‘‘control compliance’’ approach. Through the RMA, the Department effectively and efficiently meets its obligations under the Federal Information Security Management Act (FISMA) in a manner that improves, rather than impedes, the fulfillment of the Department’s statutory missions.

The CSP, through DOE’s RMA:

- a. establishes line management accountability for ensuring protection of information and information systems through Federal DOE Management (FDM) consisting of the Department’s Under Secretaries, the Energy Information Administration, Power Marketing Administrators and the Chief Information Officer (CIO) (see attachment 2 for a pictorial representation of DOE 1204).
- b. recognizes the Department’s federated government-owned contractor operated (GOCO) environment and appropriately integrates cyber security governance, accountability and reporting into management and work practices at all levels of the Department.
- c. institutes a matrix-centric, risk-based approach to the management of cyber security to ensure the confidentiality, integrity, and availability of DOE information and information systems;
- d. requires a training, education, and awareness program that develops and maintains cyber security competencies including threat identification and risk management throughout DOE Federal and contractor workforce that enables personnel to fulfill their responsibilities in protecting DOE information and information systems;
- e. establishes cyber security governance processes that are mission-focused;
- f. defines enterprise-level cyber security requirements, processes and responsibilities for the governing executive and national security information and information systems, and

AVAILABLE ONLINE AT: [www.doe.gov/40401](http://www.doe.gov/40401) INITIATED BY: Office of the Chief Information Officer



Office of Environmental Management (EM)  
Cyber Security Policy and  
Risk Management Approach Implementation  
Plan  
February 2014



Office of Environmental Management  
U.S. Department of Energy  
Washington, DC

DOE EM 264-13 1 of 24





# The System Security Plan (SSP)

## The System Security Plan Describes:

- System/system accreditation boundary
- Information types and the confidentiality, integrity, and availability requirements for each
- System categorization
- Baseline set of cyber security controls
- How each control is implemented by the system
  - System environment [physical, logical (networking, etc.), and operational] and identifies
    - Environment unique threats/vulnerabilities
    - Countermeasures (special security controls)
- System interconnections and signed agreements





# Key Policy & Guidance Documents

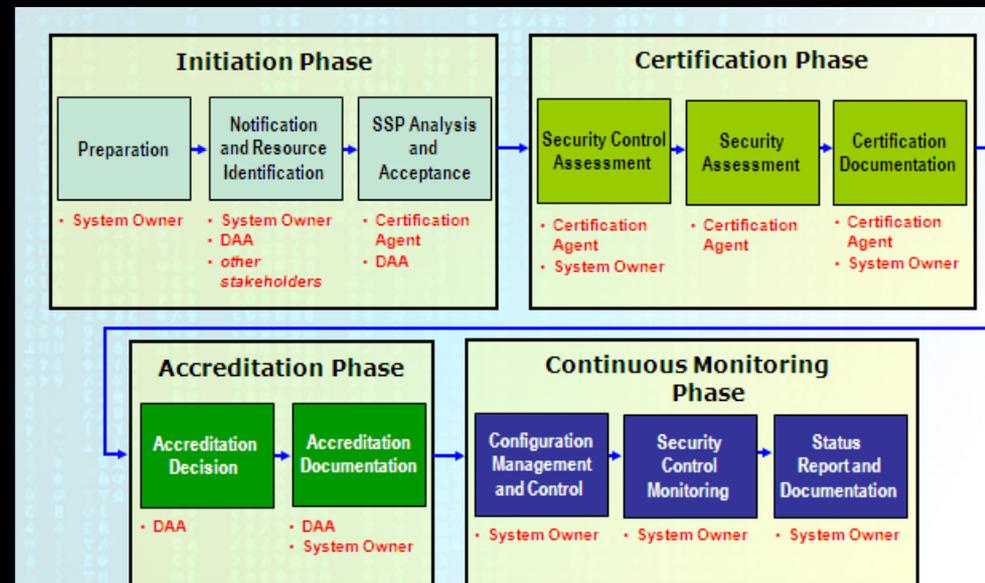
- **National Institute of Standards and Technology (NIST) 800-18 Rev 1, *Guide for Developing Security Plans for Federal Information Systems*;**
- **National Institute of Standards and Technology 800-37 Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*;**
- **National Institute of Standards and Technology 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;**
- **National Institute of Standards and Technology 800-137, *Information Security Continuous Monitoring (ISCM)*;**
- **DOE Environmental Management (DOE-EM) *Risk Management Approach Implementation Plan (RMAIP)*;**
- **NIST FIPS Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems*;**  
and
- **DOE order 205.1B, *Department of Energy Cyber Security Program*.**





# Certification & Accreditation

- Used when launching a new system
- Used when major changes take place to an existing system





# C&A Life Cycle

## Initiation Phase

Preparation

- System Owner

Notification and Resource Identification

- System Owner
  - AO
  - other stakeholders

SSP Analysis and Acceptance

- Certification Agent
  - AO

## Certification Phase

Security Control Assessment

- Certification Agent
- System Owner

Security Assessment

- Certification Agent

Certification Documentation

- Certification Agent
- System Owner

## Accreditation Phase

Accreditation Decision

- AO

Accreditation Documentation

- AO
- System Owner

## Continuous Monitoring Phase

Configuration Management and Control

- System Owner

Security Control Monitoring

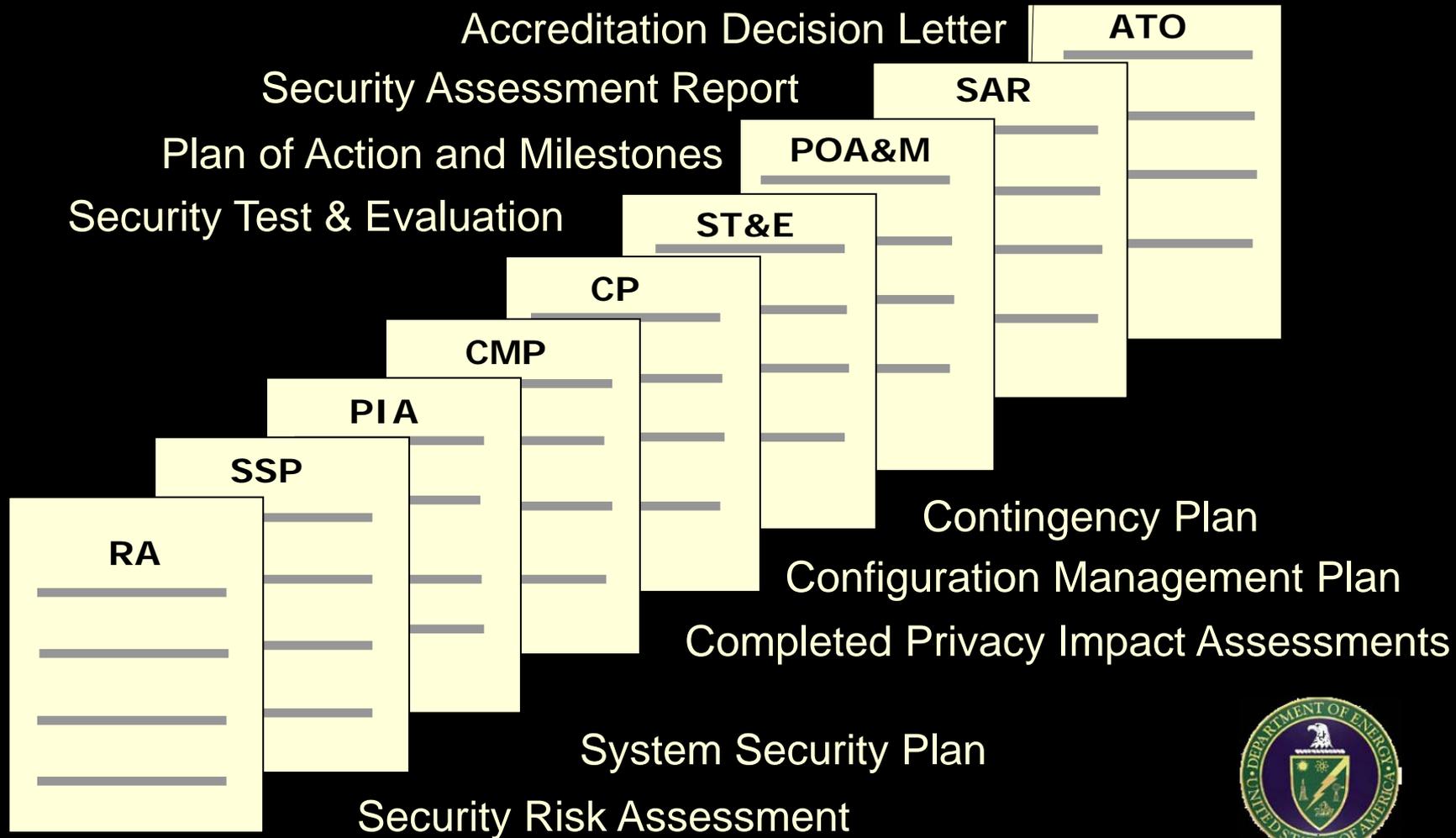
- System Owner

Status Report and Documentation

- System Owner



# The Completed C&A Package





# Policy - RMAIP

- Recognizes that the EM mission and business processes are dependent on the sites information technology (IT) infrastructure for the completion of the DOE mission
- The old PCSP was very prescriptive, demanded 154 NIST controls
- The RMAIP allows greater flexibility to tailor controls out when they are no longer applicable
- Waivers and exceptions are no longer needed
- No need to spend more on protections than the value of the system

---

Office of Environmental Management (EM)  
Cyber Security Policy and  
Risk Management Approach Implementation  
Plan  
February 2014

---



Office of Environmental Management  
U.S. Department of Energy  
Washington, DC

---



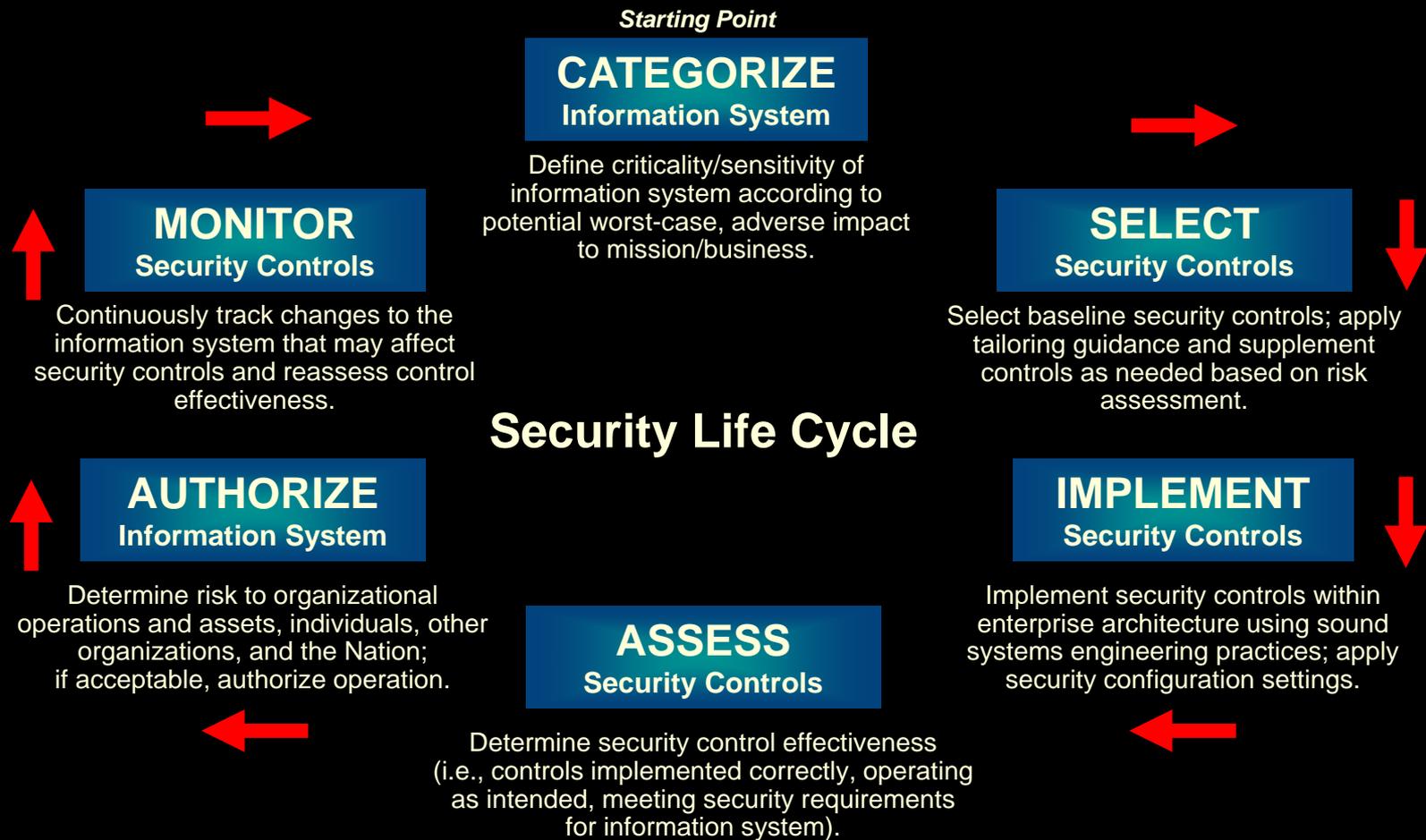
# Continuation of Continuous Monitoring

- **Recognition that signature based protection programs, annual assessments and three-year static certification and accreditation processes are no longer effective in safeguarding IT assets and data**
- **Only active monitoring of security controls can prevent or address the detection, analysis, eradication and timely incident response activities to these attacks**
- **The use of Continuous Monitoring means that sites are expected to be proactive in meeting these new threats, vulnerabilities and attacks without waiting for contractual changes in their respective contracts**





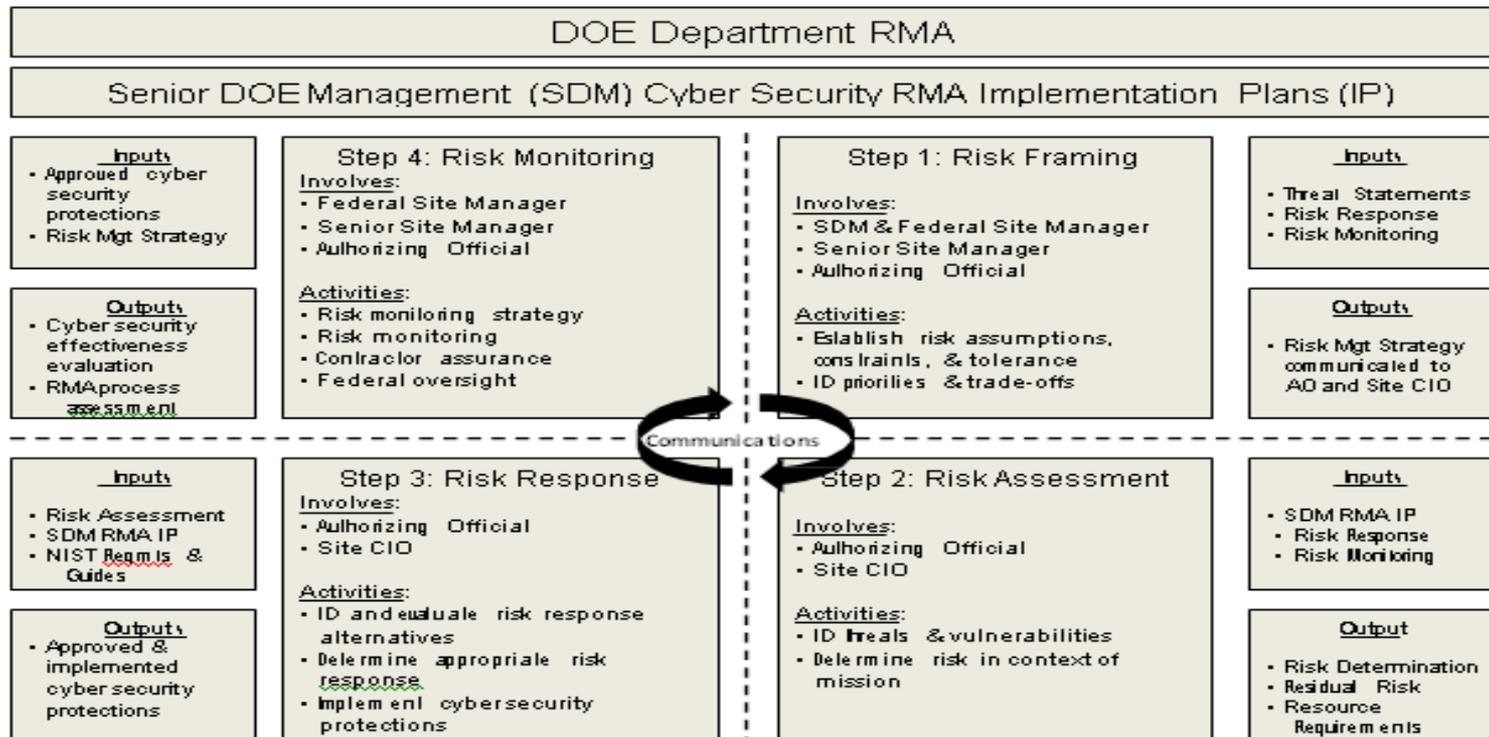
# Risk Management Framework





# The RMA Process

## DOE Risk Management Approach (RMA) Process





# Risk Management Framework

*Starting Point*

## CATEGORIZE Information System

Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.

**RMA Step 1  
Risk Framing**

## SELECT Security Controls

Select baseline security controls, tailoring guidance and supplementary controls as needed based on risk assessment.

**RMA Step 2  
Risk Assessment**

## IMPLEMENT Security Controls

Implement security controls, enterprise architecture using systems engineering practices, apply security configuration settings.

**RMA Step 3  
Risk Response**

## ASSESS Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements for information system).

## MONITOR Security Controls

Continuously track changes to the information system that may affect security controls and reassess control effectiveness.

**RMA Step 4  
Risk Monitoring**

## AUTHORIZE Information System

Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.

### Security Life Cycle





# NIST 800-53 Controls

NIST Special Publication 800-53  
Revision 4

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

Security and Privacy Controls  
for Federal Information Systems  
and Organizations

JOINT TASK FORCE  
TRANSFORMATION INITIATIVE

## INFORMATION SECURITY

INITIAL PUBLIC DRAFT

Computer Security Division  
Information Technology Laboratory  
National Institute of Standards and Technology  
Gaithersburg, MD 20899-8930

February 2012



U.S. Department of Commerce  
John K. Bryson, Secretary

National Institute of Standards and Technology  
Patrick D. Gallagher, Under Secretary for Standards and Technology  
and Director





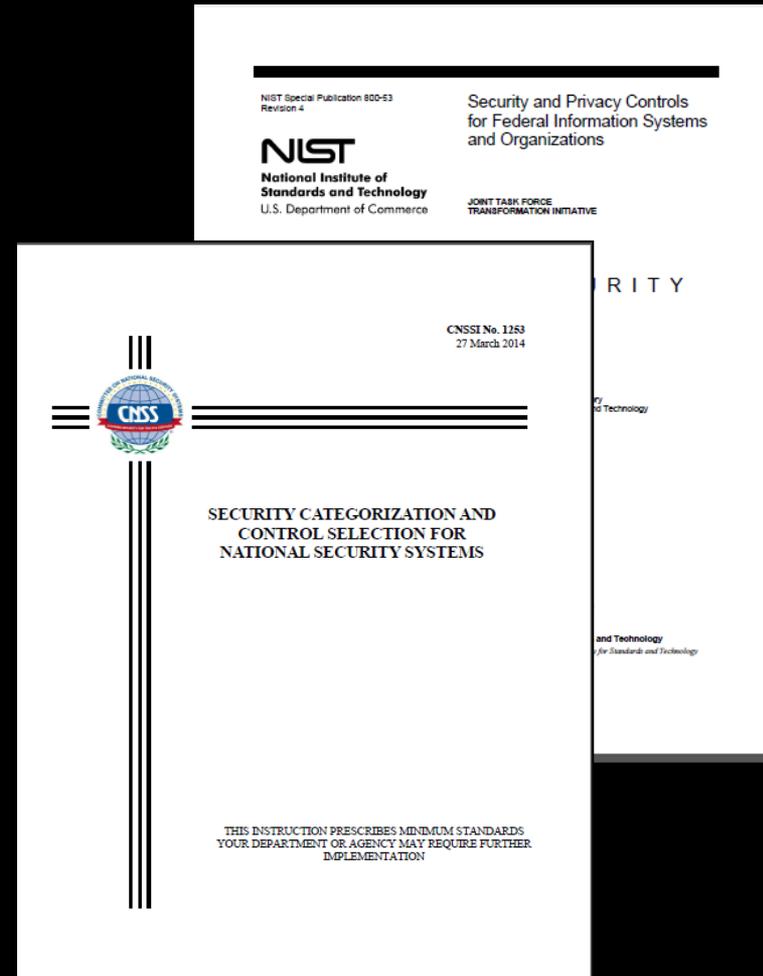
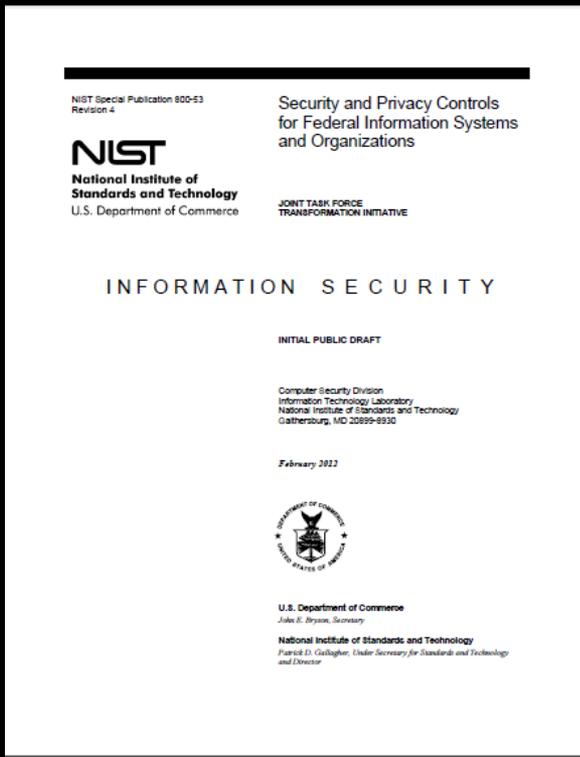
# 18 Families

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management





# Defined Guidance for Both Types

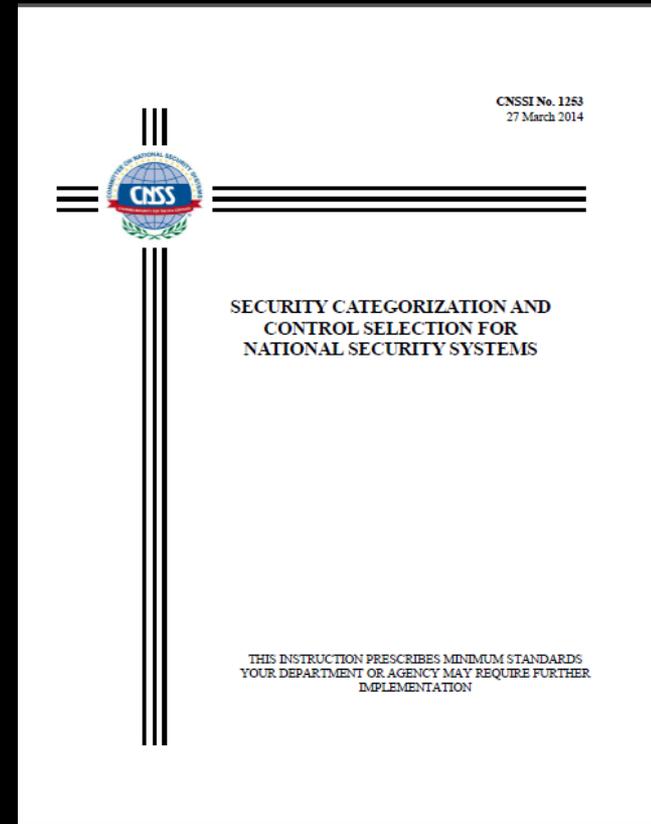




# Classified Systems

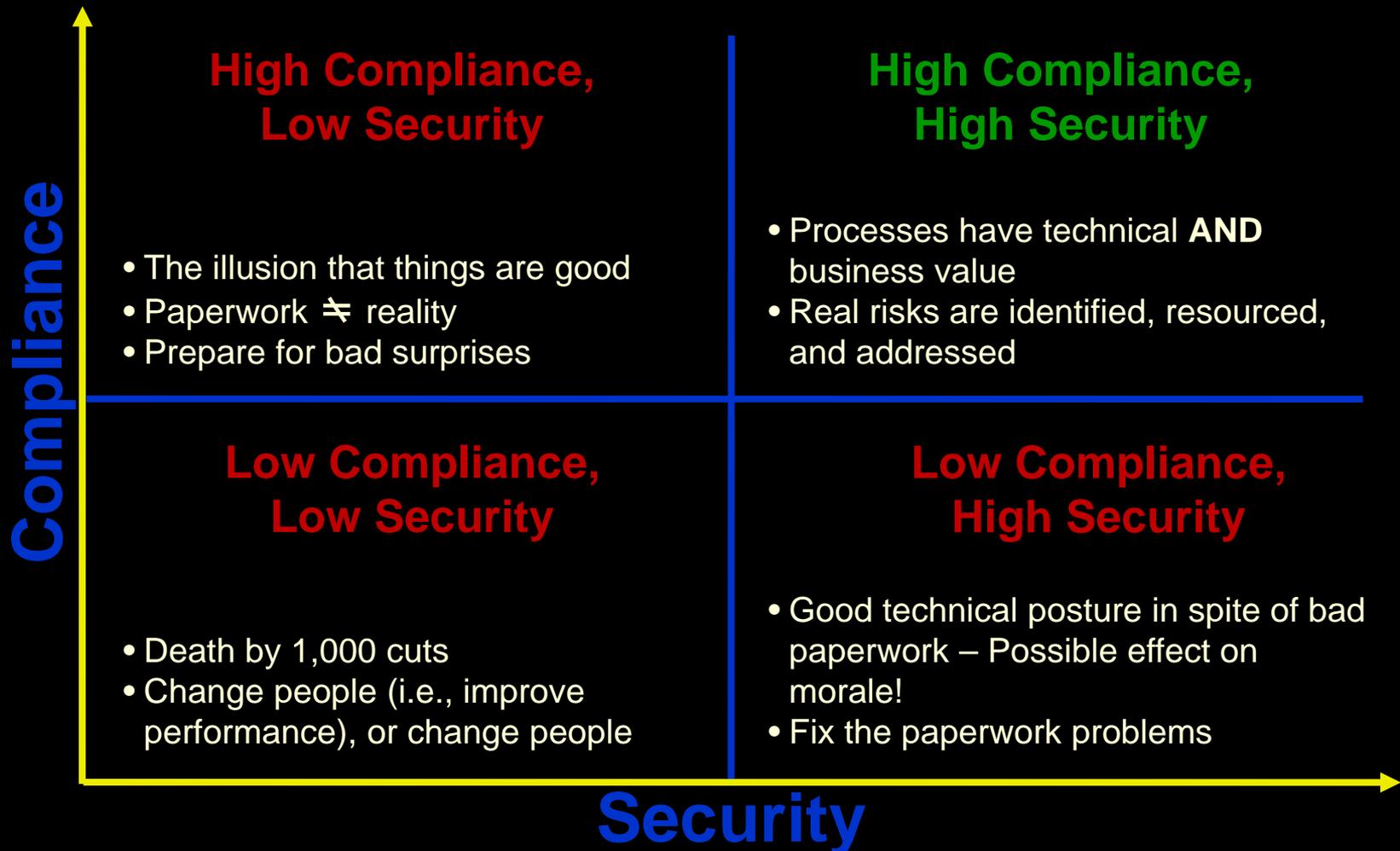
## Key Differences with Unclassified System

- Higher level of responsibility and risk
- Higher level of rigor in protection
- Level of support in protection is critical
- Additional Guidance:
  - Committee on National Security Systems Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems*
- No Penetration Testing performed
- Insider threat assessment performed





# Compliance and Security are Different Things





# The MIPP Mission

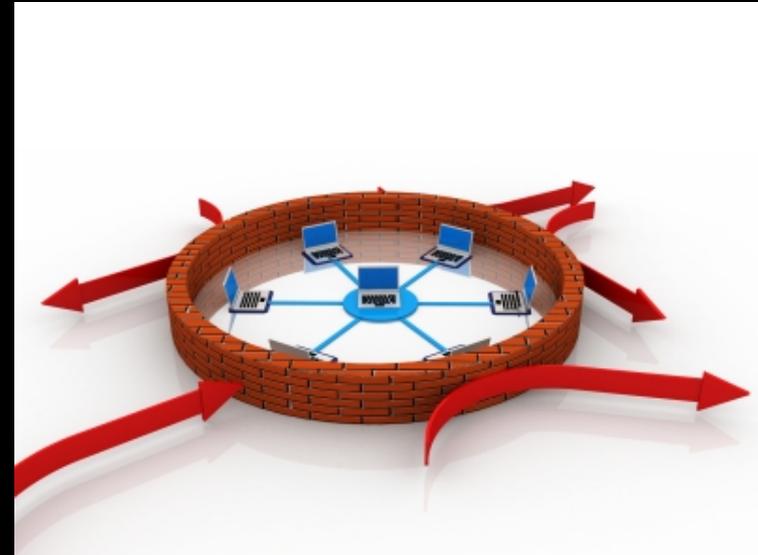
Site Assistance	Independent Security Test and Evaluation	Continuous Monitoring	POA&M Validation and Verification	Cyber Security Monitoring
Assist EM sites in preparation of documentation for systems	Perform independent ST&E and Security Assessment Reports (SAR)	Perform CM Assessments and Penetration testing	Perform POA&M validation and verification functions	Organizational incident reporting, analysis, eradication and network protection monitoring

Your success is our only goal!



# Purpose of CM

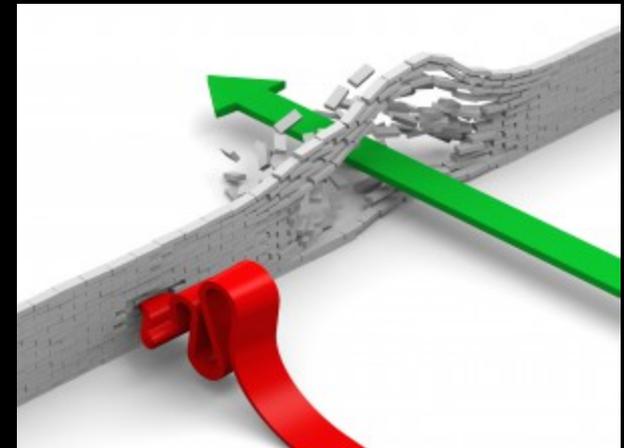
- Support the Authority to Operate (ATO)
  - “Snapshot” in time
    - Is the risk level the same?
    - Is it acceptable?
  - Change happens
    - Configuration Management
    - Vulnerabilities, patches,
    - New HW/SW/applications, etc...
    - New threats
  - Continuous Monitoring
    - Maintaining security controls at acceptable levels of Risks daily!





# Purpose of Penetration Testing

- Conduct network and application Pen Testing
- Look for vulnerabilities that can be exploited and “exploit them in a controlled manner”
- Make the site aware of real vulnerabilities and real exploits so corrective action can be taken “now”
- Recommend solutions for validated vulnerabilities and prioritize them





# Process for Resolving Differences

- Applies to CM & Pen Testing activities
  - Discussion of differences of opinion
  - Document as appropriate
    - What is the difference?
    - What we all agree with?
    - What we all disagree with?
    - List possible solutions?
    - List recommendations?
  - CSPM reviews and comments with his/her decision
  - AO/ AODR discussion and decision if needed (final)





# On-Site Planned Activities

Activities (2014)	Selected (Yes or No)
Continuous Monitoring	Yes
Incident Response Test or Exercise	Yes
Contingency Plan Test or Exercise	Yes
Compliance Scanning (Baseline)	Yes
Penetration Testing	Yes
Phishing Test	Planned
Others as documented in the Site Assistance Plan	Yes (as time permits)



# Q&A

