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

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

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.
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

Legend:
- **DOE Organization**
- **Federal employee role**
- **Role that may be held by Contractor**
- **Direct accountability**
- **Reporting/informational relationship**

AO

DOE Under Secretary’s Office

Program Office HQ

Energy CSPM

DOE Site Manager’s Organization

Program Office CSPM

ISSOs

ISSM

System Owners

SCA

AODR
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

- FISMA Law
- OMB Direction (Circular A-130, Memoranda, etc)
- DOE Sec/DepSec/UnderSec Memoranda
- DOE Order 205.1B
- EM-1/EM-2 Memoranda
- EM RMAIP
- System Security Plan
- Local Site Procedures
The Policy Hierarchy

- **FISMA Law**
- **Presidential Directives**
  - **Executive Orders**
- **OMB Memoranda and Circulars**
- **CNSS Guidance**
- **NIST Guidance**

**What**
- **DOE Policies and Orders**
  - **DOE Deputy Secretary**
  - **Senior DOE Managers**
  - **Operating Unit Manager**

**How**
- **Risk Management Approach**
- **Cyber Security Program Plan**
  - **System Security Plan (Living Document)**
- **System Owner**
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
• **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
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
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
• 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)
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
(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

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
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 800-137, *Information Security Continuous Monitoring (ISCM)*;
- DOE Environmental Management (DOE-EM) *Risk Management Approach Implementation Plan (RMAIP)*;
- 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
  - AO
  - System Owner
- **Security Assessment**
  - Certification Agent
  - System Owner
- **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
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
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

Security Life Cycle

Starting Point

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

SELECT
Security Controls
Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

IMPLEMENT
Security Controls
Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.

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

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

MONITOR
Security Controls
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.
Risk Management Framework

Security Life Cycle

**CATEGORIZE**
Information System

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

**SELECT**
Security Controls

Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.

**IMPLEMENT**
Security Controls

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

**ASSESS**
Security Controls

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

**AUTHORIZE**
Information System

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

**MONITOR**
Security Controls

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

**RMA Step 1**
Risk Framing

**RMA Step 2**
Risk Assessment

**RMA Step 3**
Risk Response

**RMA Step 4**
Risk Monitoring
<table>
<thead>
<tr>
<th>ID</th>
<th>FAMILY</th>
<th>ID</th>
<th>FAMILY</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Access Control</td>
<td>MP</td>
<td>Media Protection</td>
</tr>
<tr>
<td>AT</td>
<td>Awareness and Training</td>
<td>PE</td>
<td>Physical and Environmental Protection</td>
</tr>
<tr>
<td>AU</td>
<td>Audit and Accountability</td>
<td>PL</td>
<td>Planning</td>
</tr>
<tr>
<td>CA</td>
<td>Security Assessment and Authorization</td>
<td>PS</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>CM</td>
<td>Configuration Management</td>
<td>RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>CP</td>
<td>Contingency Planning</td>
<td>SA</td>
<td>System and Services Acquisition</td>
</tr>
<tr>
<td>IA</td>
<td>Identification and Authentication</td>
<td>SC</td>
<td>System and Communications Protection</td>
</tr>
<tr>
<td>IR</td>
<td>Incident Response</td>
<td>SI</td>
<td>System and Information Integrity</td>
</tr>
<tr>
<td>MA</td>
<td>Maintenance</td>
<td>PM</td>
<td>Program Management</td>
</tr>
</tbody>
</table>
Defined Guidance for Both Types
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:
• No Penetration Testing performed
• Insider threat assessment performed
Compliance and Security are Different Things

High Compliance, Low Security
- The illusion that things are good
- Paperwork ≠ reality
- Prepare for bad surprises

High Compliance, High Security
- Processes have technical AND business value
- Real risks are identified, resourced, and addressed

Low Compliance, Low Security
- Death by 1,000 cuts
- Change people (i.e., improve performance), or change people

Low Compliance, High Security
- Good technical posture in spite of bad paperwork – Possible effect on morale!
- Fix the paperwork problems
## The MIPP Mission

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

*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

<table>
<thead>
<tr>
<th>Activities (2014)</th>
<th>Selected (Yes or No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous Monitoring</td>
<td>Yes</td>
</tr>
<tr>
<td>Incident Response Test or Exercise</td>
<td>Yes</td>
</tr>
<tr>
<td>Contingency Plan Test or Exercise</td>
<td>Yes</td>
</tr>
<tr>
<td>Compliance Scanning (Baseline)</td>
<td>Yes</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>Yes</td>
</tr>
<tr>
<td>Phishing Test</td>
<td>Planned</td>
</tr>
<tr>
<td>Others as documented in the Site Assistance Plan</td>
<td>Yes (as time permits)</td>
</tr>
</tbody>
</table>