CSEAT Purpose

- Improve federal agency Critical Infrastructure Protection (CIP) planning and implementation efforts
- Assist agencies in improving the security of federal IT systems
  - Strengthen security of critical computer system/services
  - Identify security program issues and provide specific remedies
  - Prepare for future security threats
- Identify and develop needed computer security guidance
CSEAT Review

- Unclassified ONLY
- CSEAT provides an independent review of an agency’s IT security program or high risk program
  - Agency requested - not an audit
  - Assesses the state of maturity of the agency’s or program’s IT security policy and procedure implementation and overall integration
- CSEAT applies a consistent and comparable approach to the review
  - Consistent application of control objectives and effectiveness criteria
  - Comparable review of agency or program organizational structure, culture, etc.

CSEAT Agency Review Process

1. CSEAT conducts kickoff meeting with agency
2. Agency provides requested information
3. CSEAT reviews information and schedules interviews
4. CSEAT develops DRAFT report
5. CSEAT presents recommendations
6. CSEAT finalizes report
7. CSEAT conducts interviews
8. CSEAT presents recommendations
### Proposed Review Timeline

<table>
<thead>
<tr>
<th>Agency provides:</th>
<th>CSEAT</th>
<th>CSEAT:</th>
<th>CSEAT:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation</td>
<td>Reviews documentation and responses to questions</td>
<td>Conducts interviews</td>
<td>Writes draft review report</td>
</tr>
<tr>
<td>Response to questions</td>
<td>Schedules interviews</td>
<td>Request additional information</td>
<td></td>
</tr>
<tr>
<td>Key personnel information (within 1 week)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Timeline phase duration is dependent upon completion of previous phase.

Agency provides comments on draft – 30 days after receipt of draft
CSEAT provides final review report – 14 days after receipt of comments

---

### CSEAT Review Report

- CSEAT overview
- Agency or program overview
- Agency or program status
- Recommendations for to improve agency or program computer security
- Summary and conclusions
- Prioritized, implementable action plan
Agency IT Security Status

Computer Security Management and Culture
- IT roles and responsibilities
- Review of security controls
- Rules of behavior and documentation
- Performance assessment and feedback
- Critical infrastructure protection
- Personnel controls

Computer Security Plans
- System security plan
- Risk management
- Authorized processing
- Documentation

Security Awareness, Training, and Education
- End users’ security awareness and training
- IT professionals’ security awareness and training
- Management security awareness and training

Budget and Resources

Life Cycle Management

Incident and Emergency Response

Operational Security Controls

Physical Security

IT Security Controls

Compliant
Partially Compliant
Not Compliant

CSEAT Review Topic Subareas

Computer Security Management and Culture
- Program specific controls

Computer Security Plans
- Program specific security training

Security Awareness, Training, and Education
- Program specific security training

All Reviews

Only High Risk Program Reviews

NIST CENTENNIAL
### CSEAT Review Topic Subareas (Continued)

<table>
<thead>
<tr>
<th><strong>Budget and Resources</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• IT security part of capital planning process</td>
</tr>
<tr>
<td>• Adequate resources applied to IT security</td>
</tr>
<tr>
<td>• IT security funding and resources distributed based upon a risk model</td>
</tr>
<tr>
<td>• Cost effective IT security solutions</td>
</tr>
<tr>
<td>• Procurement controls</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Life Cycle Management</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• System development life cycle (SDLC) methodology</td>
</tr>
<tr>
<td>• Changes controlled and tested through SDLC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Incident and Emergency Response</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Critical and sensitive asset identification</td>
</tr>
<tr>
<td>• Contingency/disaster response</td>
</tr>
<tr>
<td>• Incident identification, reporting, and response</td>
</tr>
<tr>
<td>• Continuity of operations</td>
</tr>
</tbody>
</table>

### Operational Security Controls

| • Hardware and systems software maintenance |
| • Data integrity |
| • Production I/O |
| • Data confidentiality |
| • Data availability |
| • Systems operations documentation |

### Physical Security

| • Implementation of physical security controls |
| • Personal electronic device protection |
| • Emanation controls |
| • Temporary controlled facility controls |

### IT Security Controls

| • Identification and authentication |
| • Logical access controls |
| • Auditing |
Issue Identification with Corrective Actions

**Issue:** Information and systems are endangered due to a failure to manage access rights and accounts for agency employees.

**Discussion:**
Discussion of issue.

**Corrective Actions:**
Description of corrective action.

- Cost – minimal
- Time to Complete – short-term
- Recurring Cost – minimal
- Recurring Time to Complete – short-term

Prioritized Action Plan

- Priority
- Topic area
- Issue
- Corrective action
- How long to complete initial action
- Cost to complete initial action
- How long to complete recurring action
- Cost to complete recurring action
### Sample Change in Computer Security Posture after $2 Million Action Plan

**CSEAT Review Areas**
1. Computer Security Management and Culture
2. Computer Security Plans
3. Security Awareness, Training, and Education
4. Budget and Resources
5. Life Cycle Management
6. Incident and Emergency Response
7. Operational Security Controls
8. Physical Security
9. IT Security Controls

#### Current Status

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Computer Security Enhancements
- Complete policies
- Complete procedures
- Increase documentation
- Develop and implement capital planning process
- Augment employee training
- Implement computer security plans
- Develop risk assessment methodology
- Develop performance metrics

#### $2 M Invested

**CSEAT Uses Report to Develop Guidance**

- Sanitized Case Study
- NIST Guidance
- CSEAT Review Report with Recommendations
Common Issues

- Lack of formalization
  - Bob knows how to do it
  - Alice keeps the server secure
  - We all know what has to be done and don't need it written down

- Impact
  - Single point of failure
  - Work waits until employee returns
  - Employee retires and new person doesn't know what has been done
  - Little ability to recover from disaster

Common Issues (continued)

- Policies not defined
  - Different groups independently decide on a policy
  - Inconsistent interpretation across organization

- Impact
  - Interpretation may not reflect real organizational requirements
  - Difficult to identify the cause of problems
Common Issues (continued)

- Procedures not defined
  - Different groups perform IT security differently
  - Inconsistent implementation across organization

- Impact
  - Implementations may not reflect real organizational requirements
  - Difficult to identify the cause of problems

Common Issues (continued)

- Capital planning process missing IT security
  - IT security not addressed as a primary component
  - Performance measures not included
  - Cost-effectiveness of IT security solutions not addressed

- Impact
  - Budgets may be cut or redirected
  - Adequate resources may not be applied to IT security
  - Implemented IT security solutions may not be cost-effective
Common Issues (continued)

- **IT security considered “their” problem**
  - IT security issues provided to IT security personnel
  - IT security not integrated into all positions
  - IT security responsibility and accountability not considered part of every employee’s performance

- **Impact**
  - Critical system security may be insufficient
  - Security issues are considered to be someone else’s problem
  - Vulnerabilities increase over time
  - Security expenditures may be higher than necessary due to “faulty” integration into the life cycle management process

Common Issues (concluded)

- **Lack of sufficient training**
  - Employees don’t understand their role in IT security
  - Current threats not addressed
  - IT security not a primary concern
  - Systems not updated with current security patches

- **Impact**
  - Employees indulge in poor security practices
  - Systems vulnerable
  - New and updated systems insecure
Benefits of High Level IT Security Review

- Without the basic IT security infrastructure, it is virtually impossible to have effective IT security.
- Independent and neutral third party can more readily identify IT security issues.
- NIST has extensive knowledge of relevant legislation, standards and guidelines and can identify issues and corrective actions.
- NIST is able to provide needed guidance in a timely manner.