

Computer Security Expert Assist Team



Kathy Lyons-Burke, (301) 975-4611
kathy.lyons-burke@nist.gov
Information Technology Laboratory
<http://cseat.nist.gov>
cseat@nist.gov

ACSAC
December 2001



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



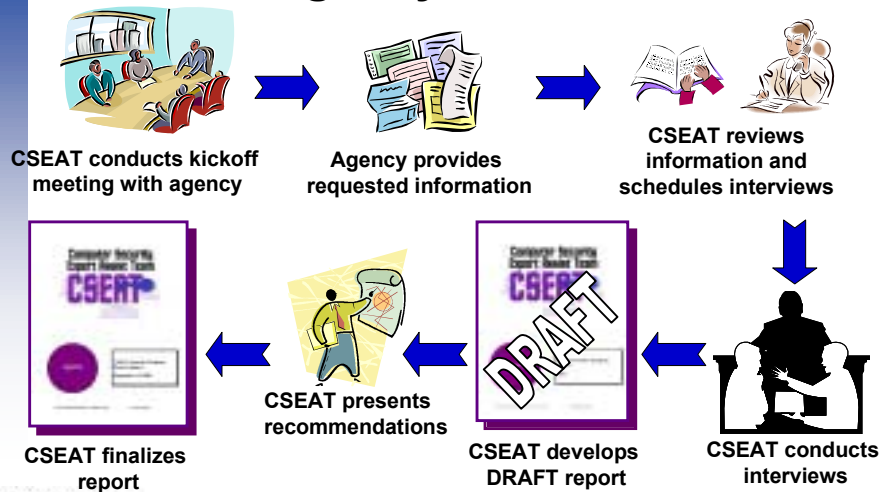
CSEAT Review

- **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.



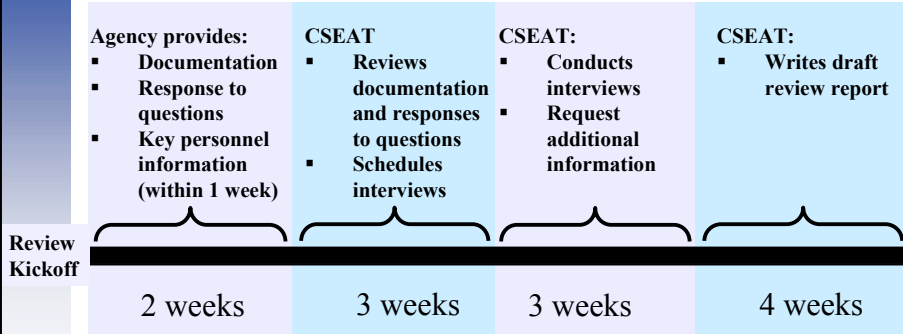
3

CSEAT Agency Review Process



4

Proposed Review Timeline



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

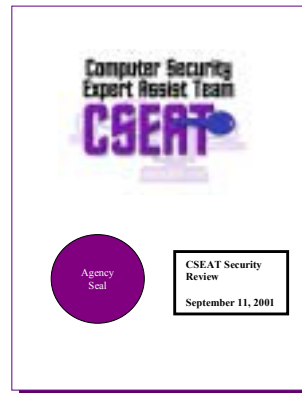


Timeline phase duration is dependent upon completion of previous phase.





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



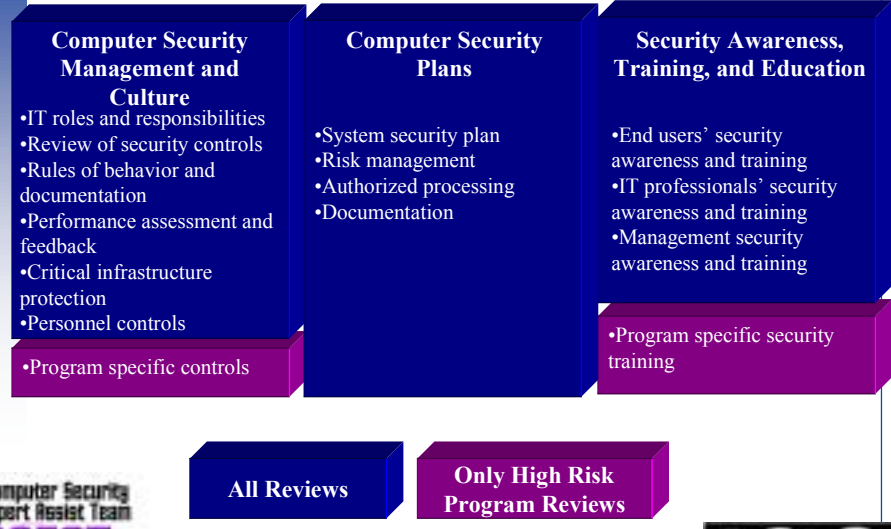
Agency IT Security Status

	Policy	Procedures	Implementation	Testing	Integration
Computer Security Management and Culture	Yellow	Yellow	Yellow	Red	Red
Computer Security Plans	Yellow	Yellow	Yellow	Red	Red
Security Awareness, Training, and Education	Green	Yellow	Yellow	Red	Red
Budget and Resources	Yellow	Yellow	Yellow	Red	Red
Life Cycle Management	Green	Green	Yellow	Red	Red
Incident and Emergency Response	Yellow	Yellow	Yellow	Red	Red
Operational Security Controls	Green	Yellow	Yellow	Red	Red
Physical Security	Yellow	Yellow	Yellow	Red	Red
IT Security Controls	Yellow	Yellow	Yellow	Red	Red

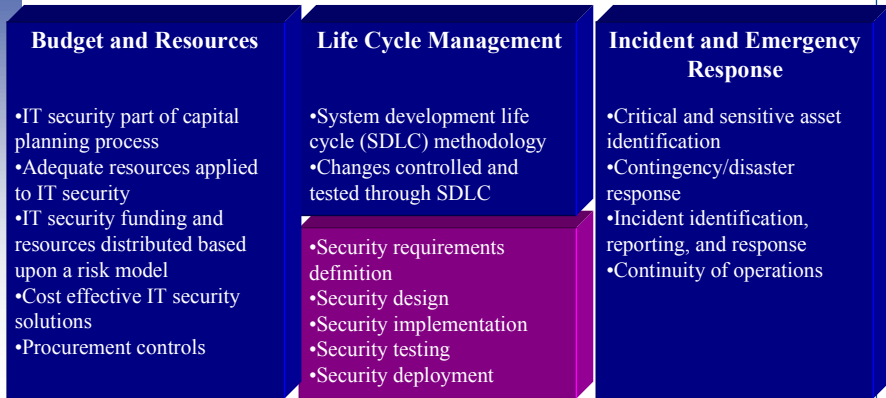
Compliant 
 Partially Compliant 
 Not Compliant 



CSEAT Review Topic Subareas



CSEAT Review Topic Subareas (Continued)

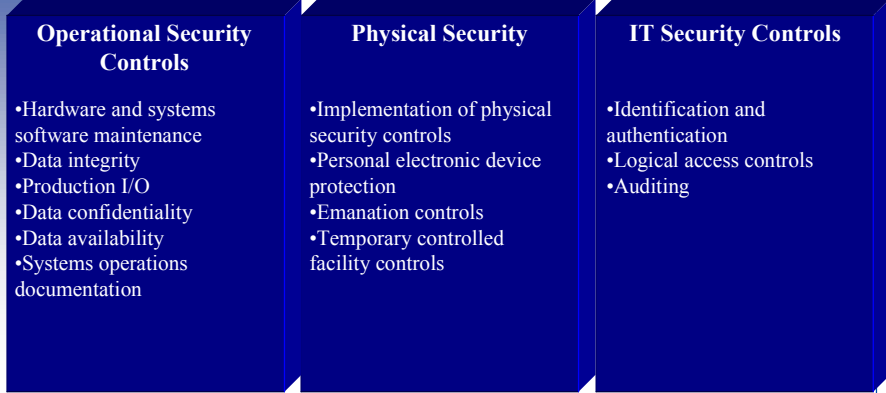


All Reviews

Only High Risk Program Reviews



CSEAT Review Topic Subareas (Concluded)



All Reviews

Only High Risk Program Reviews



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



11



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



12

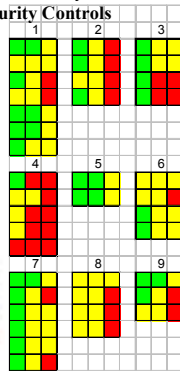


Sample Change in Computer Security Posture after \$2 Million Action Plan

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

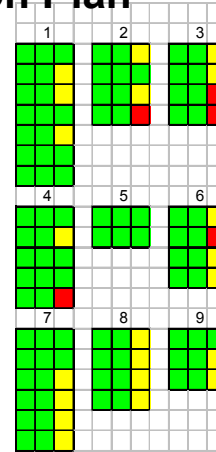


\$2 M Invested



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



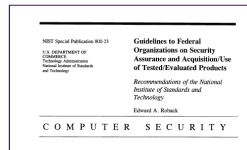
CSEAT Uses Report to Develop Guidance



CSEAT Review Report with Recommendations



Sanitized Case Study



NIST Guidance



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



15



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



16



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



17



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



18



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



19



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



20



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.

