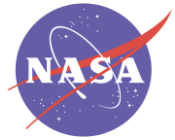


A Comprehensive Approach to Countering Security Threats

Mike Pajevski
Jet Propulsion Laboratory,
California Institute of Technology
12 June 2013

Introduction

This presentation will delve into the following topics:

- **The wide range of security threats**
- **A comprehensive approach to dealing with security threats**
- **The need for oversight & guidance**
- **Managing security risks**
- **Secure practices & strong security controls**
- **Some challenges to countering security threats**
- **Overcoming challenges to countering security threats**

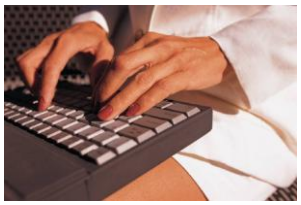
Many Security Threats

- **Space flight missions are faced with numerous security threats**

Physical Attack

Counterfeit Parts

Malicious
Sites & Content



Cyber Attack

Malware

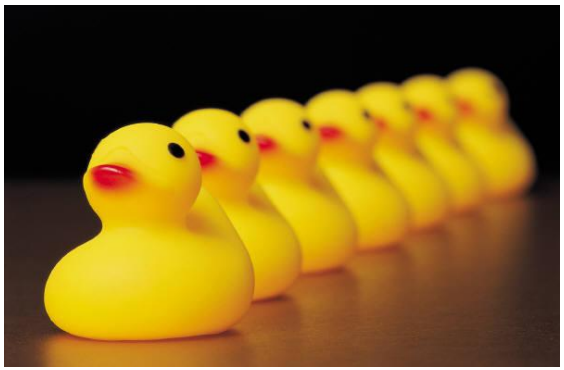
Communications Jamming,
Interception & Intrusion

Stolen Documents, Media,
Laptops, PDAs, etc.

Unauthorized
Information
Disclosure

A Comprehensive Approach

- **Question: What is a "comprehensive approach"?**
- **Answer: One that covers -**
  - **Proper oversight & guidance**
  - **Effective security risk management**
  - **Secure practices throughout a system's life cycle**
  - **Strong security controls, providing:**
    - **Prevention – stopping attacks from being successful**
    - **Detection – knowing when you've been attacked**
    - **Resilience – being able to operate even when compromised**

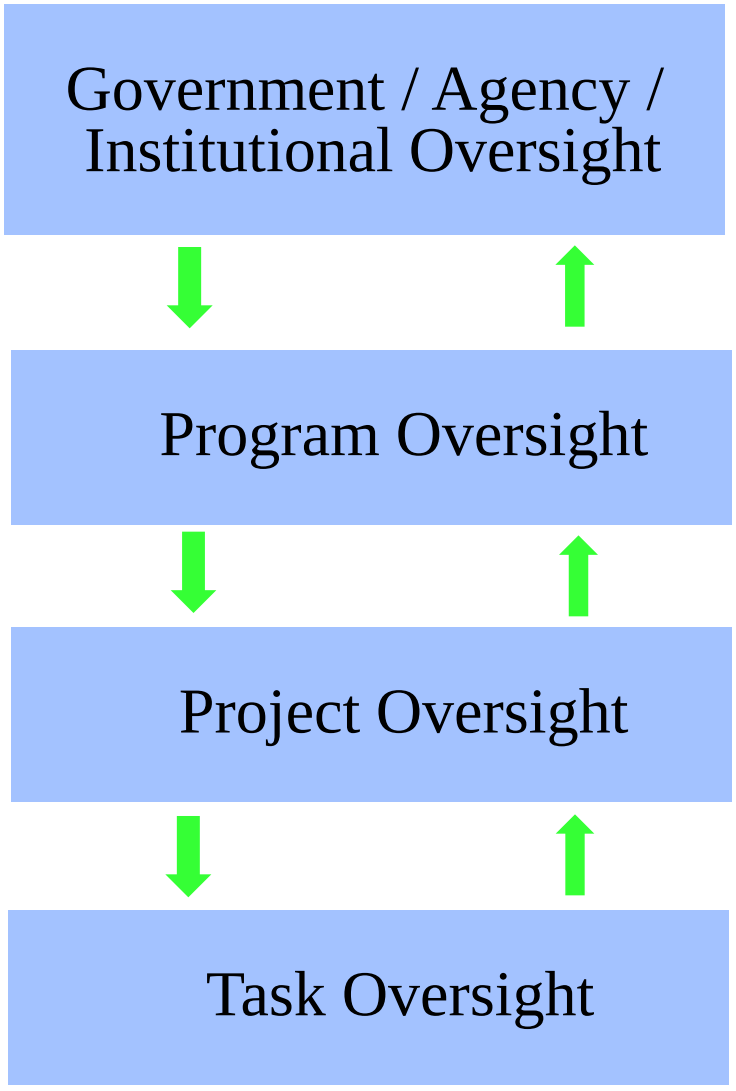


Oversight

- **Oversight = careful management & supervision**
  - **It is not simply about checklists and compliance!**
    - **Checklists are a guide, not a silver bullet**
    - **Compliance may be a requirement, but not a substitute for thinking**
- **Why is good oversight important?**
  - **Provides appropriate objectives and keeps things on track**
- **What makes good oversight?**
  - **Effective & efficient processes**
    - **Document, vet, and measure effectiveness of oversight processes**
  - **Knowledgeable people**
    - **There is no substitute for understanding**
    - **Must have appropriate knowledge & expertise at each level**
  - **Accountability**
    - **“Responsibility” & “Ownership” are key**
    - **Duties and repercussions must be clear, reasonable, & enforced**

Layered Oversight

- **Oversight is layered**
  - **More detail each level down**
- **Requirements and plans defined at each layer**
  - **Top down approach is important**
  - **Else Programs/Projects don't start with complete security objectives**
- **Reviews conducted at each level**
  - **Based on defined objectives**
  - **Use informal and formal reviews**
  - **Document inputs, results, and action items**



Guidance

Good guidance in all areas promotes better security

- **Management guidance**
  - **Security threats, mitigations, and management responsibilities**
- **Acquisition guidance**
  - **Supply chain issues, appropriate standard clauses, etc.**
- **Systems engineering guidance**
  - **Good security requirements, concepts, and design patterns**
- **Developer guidance**
  - **Secure development practices & design patterns**
- **Validation & verification guidance**
  - **Security objectives and modeling of security mechanisms**
  - **Verification techniques for functionality & vulnerabilities**
- **Operator guidance**
  - **Secure operation & recognizing/reporting/handling incidents**

Managing Security Risk

NIST & ISO define processes for managing security risks

- **Reference NIST SP 800-30 Rev. 1, NIST SP 800-39, ISO/IEC 27005:2011**

•Prepare for the assessment

- **Define purpose, scope, assumptions, constraints, info sources, and models**
- **Good preparation is key to having effective results**

•Conduct the assessment

- **Identify threats & vulnerabilities – thoroughness is key to effectiveness**
- **Determine likelihood & consequences; combine to determine risks**

•Communicate and share risk assessment information

- **Knowledge of security risks is essential to effective risk reductions**

•Maintain the risk assessment

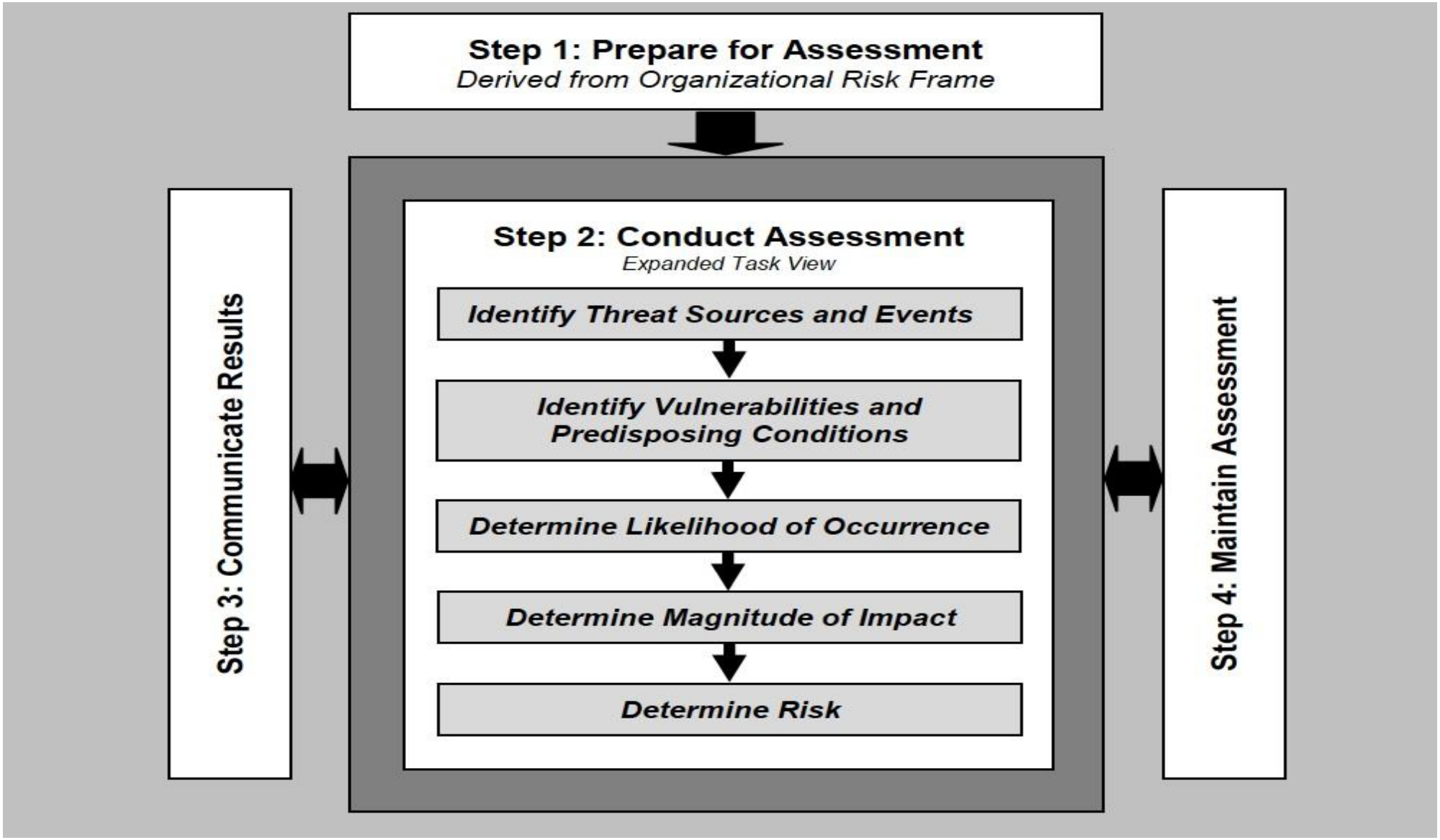
- **Keeping the assessment up-to-date is also key to effective risk mgmt**

You can’t manage what you don’t know about

- **Identifying security risks is the first step in addressing them**
- **A broad understanding of security risks supports their prioritization**
- **Don’t wait until the system is built to start assessing your security risks**

NIST Risk Mgmt Process

From NIST Special Publication (SP) 800-30 Revision 1:



NIST = National Institute of Standards & Technologies

Secure Practices

Security is a consideration in processes throughout the life cycle
- **Reference NIST SP 800-61, NIST SP 800-64, ISO/IEC 27000:2009**

- **Think about security when defining operations concepts**
  - **Who will be involved in the missions; and how does that affect security?**
  - **How do different approaches (alternatives) alter security of the system?**
- **Construct a good set of security requirements**
  - **Involve security experts in the creation of system security requirements**
  - **Consider the broad range of security issues**
  - **Make sure requirements are clear, reasonable, and verifiable**
- **Provide secure environments**
  - **For design, development, verification, and operations**
- **Follow secure acquisition and development practices**
  - **Utilize security design patterns, secure coding standards, code analysis tools, configuration mgmt**
  - **Include security clauses in acquisition contracts & screen bought components for security issues**
- **Validate & verify**
  - **For all types of security requirements**
  - **Verify functionality and look for vulnerabilities**
- **Deploy securely**
  - **Considering the people, processes, and environments involved in the deployment**
- **Operate securely**
  - **Make sure operators are trained to recognize and respond to security incidents**
  - **Define and follow contingency plans that take security issues into account**

Strong Security Controls

The wide range of security controls must be effective
- **Reference NIST SP 800-53 Rev. 4, ISO/IEC 27000:2009, ISO/IEC 27001:2005**

•Physical security
- **Guards, gates, surveillance cameras, locks, secure data centers, etc.**

•Personnel security
- **Background checks for sensitive positions**
- **Training to ensure knowledgeable and thoughtful approach to security**

•Network security
- **Firewalls up-to-date, properly configured, uncircumventable**
- **Network devices configured according to security best practices**
- **Zoned network architecture & traffic filtering**

•Secure communications
- **Virtual private networks (VPNs) & secure application layer protocols – properly configured**
- **Secure space communications – providing integrity (essential) and confidentiality (as needed)**

•Access management
- **Design applications for granular access to interfaces/information**
- **Define and enforce authorization policies that reflect real-world policies**
- **Use strong authentication mechanisms for critical functions**

•Security monitoring
- **Intrusion detection**
- **Security logging, auditing, alerting, and reporting**
- **System and security control diagnostics**

A Few Big Challenges

- **Limited resources**
  - **Limited funding and time to conduct assessment**
  - **Security expertise is in limited supply**
- **Wide range of security issues**
  - **Physical security, personnel security, cyber security**
- **Keeping up in the race**
  - **Impossible to "stay one step ahead"**
  - **Operational realities make it even harder to keep systems up-to-date**
    - **Difficult to patch systems that must operate continuously**
- **Poor/missing requirements & incomplete verification**
  - **Should start defining security requirements early; not as a bolt-on**
  - **Proper verification is necessary to measure effectiveness**
- **Misconceptions**
  - **We are safe because we have a firewall**
    - **Firewalls have vulnerabilities too & are not a panacea**
    - **What happens if the firewall is breached?**
  - **We haven't had a problem so far**
    - **How would you know? Are you looking?**

Addressing the Challenges

- **Deal with limited resources**
  - **Prioritize security risk reduction based on a thorough understanding of the risks, policies, available resources, and risk tolerance**
  - **Grow your organization - train people that support risk management**
- **Consider wide range of risks; but focus on key aspects**
  - **Delegate security responsibilities across the organization**
  - **Wide involvement in security risk assessments and reduction planning**
- **Stay current**
  - **Develop a process for identifying, incorporating, and testing patches**
  - **Maintain security awareness through continuous training & education**
- **Be thorough (and reasonable) in your security requirements**
  - **Make sure requirements are complete, clear, and verifiable**
- **Eliminate misconceptions through training & education**
  - **Don’t underestimate the importance of a good understanding of security**
  - **Essential for all levels of an organization to be free of misconceptions**

Summary

- Space flight systems are faced with various security threats
- Oversight is important to proper management of security risks
- Guidance is an important part of resolving security risks
- Risk Management is the process for identifying, analyzing, and resolving (accepting/mitigating/watching) security risks
- Secure practices are important throughout a system's lifecycle
- Strong controls are necessary to counter security threats
  - Providing "prevention", "detection", and "resiliency"
- System owners must deal with challenges such as limited resources, a wide range of security risks, evolving security risks, poor/missing security requirements, and security misconceptions

References

- **International standards:**
  - **ISO/IEC 27000:2009, Information security management systems — Overview and vocabulary**
  - **ISO/IEC 27001:2005, Information security management systems — Requirements**
  - **ISO/IEC 27005:2011, Information security risk management**

- **NIST Special Publications:**
  - **NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessments**
  - **NIST SP 800-39, Managing Information Security Risk**
  - **NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations**
  - **NIST SP 800-61, Computer Security Incident Handling Guide**
  - **NIST SP 800-64, Security Considerations in Information System Development Life Cycle**

Acronyms

- **IEC – International Electrotechnical Commission**
- **ISO – International Organization for Standardization**
- **NIST – National Institute of Standards and Technologies**
- **SP – Special Publication**

Questions?