

TACIT Security

Institutionalizing Cyber Protection for Critical Assets

Joint Federal Cyber Summit

December 4, 2013

Dr. Ron Ross

Computer Security Division

Information Technology Laboratory

Some initial thoughts.

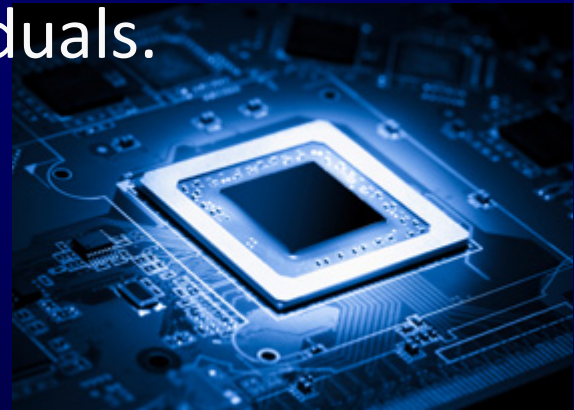


The United States Constitution

“WE THE PEOPLE of the United States, in Order to form a more perfect Union, establish Justice, ensure domestic Tranquility, *provide for the common defence*, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America...”

- We are living in the *golden age* of information technology.
- Ironically, the same information technology that has brought unprecedented innovation and prosperity to millions, has now become a significant vulnerability to nation states, corporate entities, and individuals.

How do we provide for the common defense in the digital age?



- We are vulnerable because our information technology is **fragile** and **susceptible** to a wide range of threats including:

- natural disasters;
- structural failures;
- cyber attacks; and
- errors.





Advanced Persistent Threat

An adversary that —

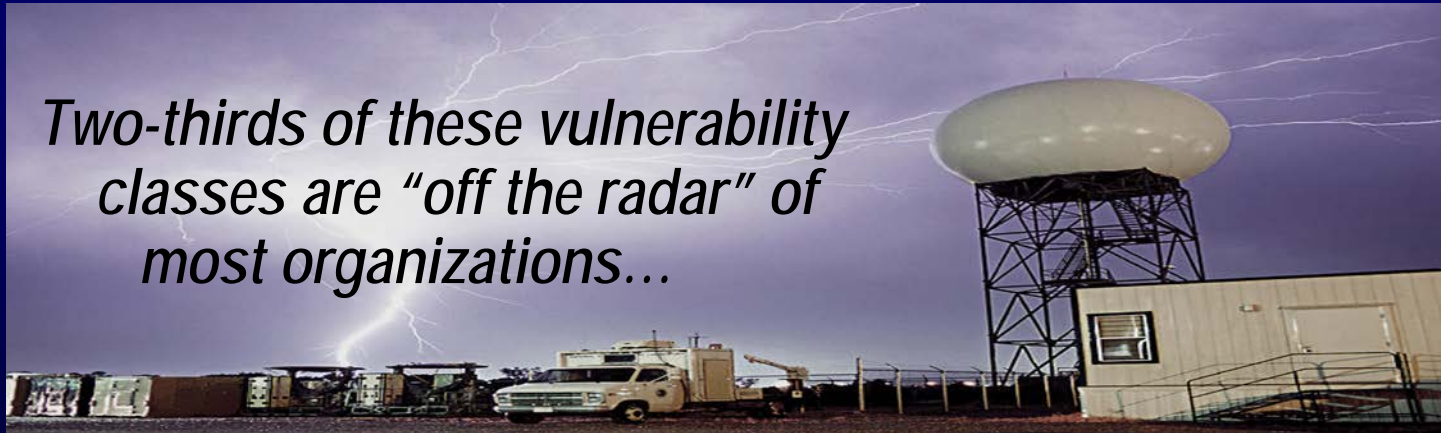
- Possesses significant levels of expertise / resources.
- Creates opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, deception).
- Establishes footholds within IT infrastructure of targeted organizations:
 - To exfiltrate information;
 - To undermine / impede critical aspects of a mission, program, or organization; and
 - To position itself to carry out these objectives in the future.

Classes of Vulnerabilities

A 2013 Defense Science Board Report described—

- **Tier 1:** Known vulnerabilities.
- **Tier 2:** Unknown vulnerabilities (zero-day exploits).
- **Tier 3:** Adversary-created vulnerabilities (APT).

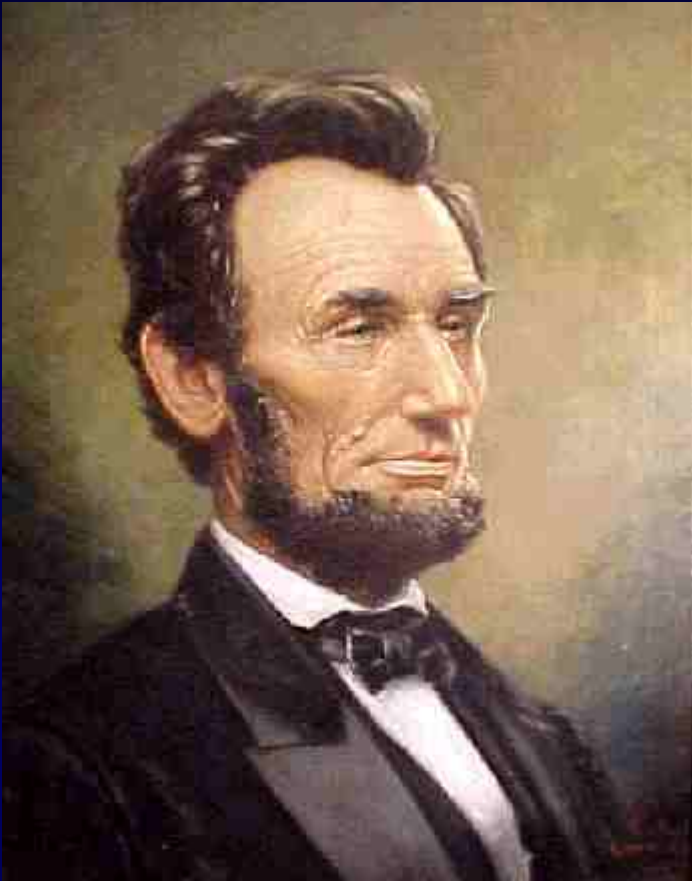
Two-thirds of these vulnerability classes are “off the radar” of most organizations...



You can't stop hurricanes...



and you can't stop cyber attacks.



Time for an honest
discussion.

Good cyber hygiene
is necessary...
But not sufficient.

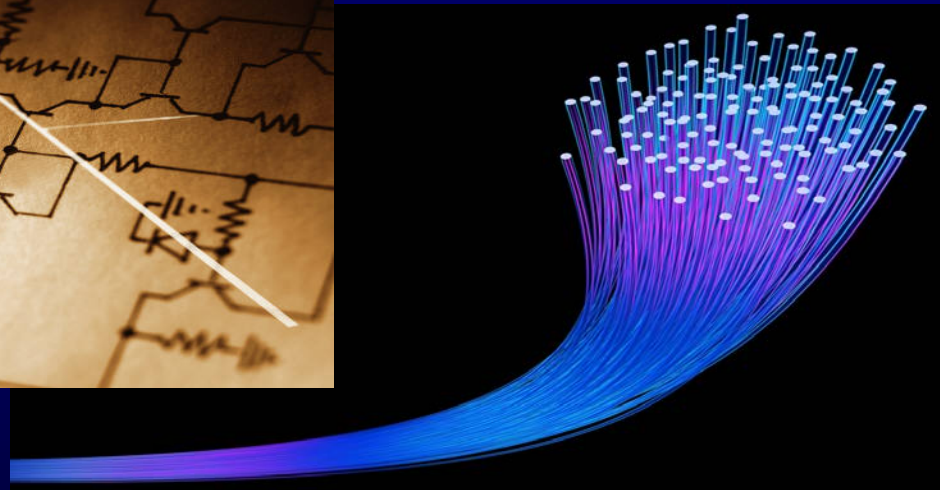


*You can't count, configure, or patch your way
out of this problem space.*

Tough decisions ahead.

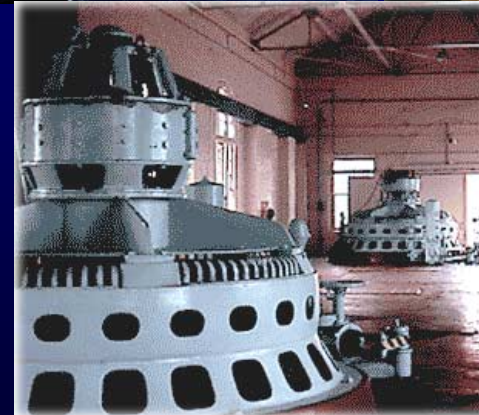
The United States Federal Cyber Security Strategy...

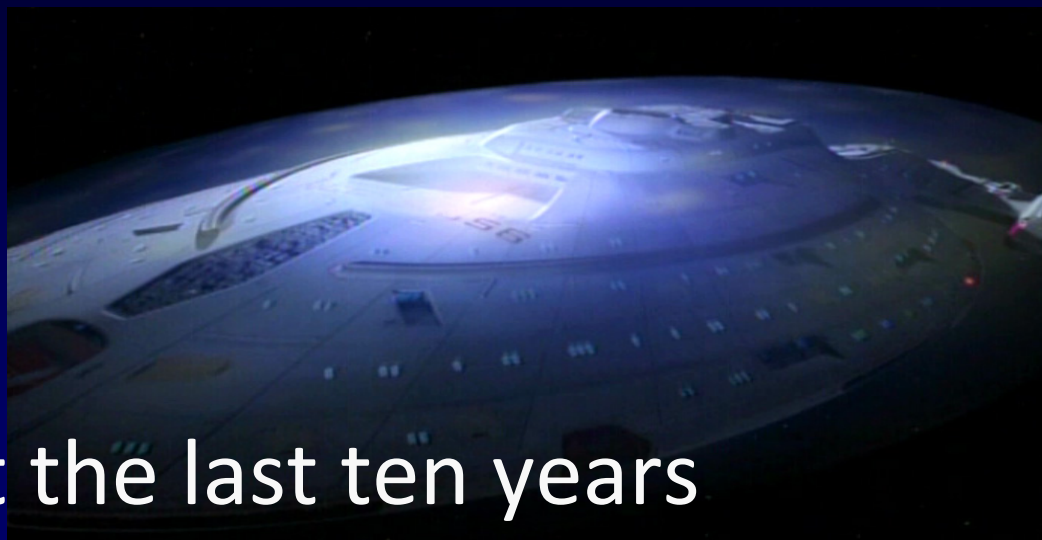
Build It Right, Continuously Monitor



The Cyber Security Toolset

- **NIST Special Publication 800-39**
*Managing Information Security Risk:
Organization, Mission, and Information System View*
- **NIST Special Publication 800-30**
Guide for Conducting Risk Assessments
- **NIST Special Publication 800-37**
*Applying the Risk Management Framework
to Federal Information Systems*
- **NIST Special Publication 800-53**
*Security and Privacy Controls for Federal
Information Systems and Organizations*
- **NIST Special Publication 800-53A**
*Guide for Assessing the Security Controls
in Federal Information Systems and Organizations*





We have spent the last ten years developing and refining our information security *toolset* but have not focused on the most effective ways to use the tools, techniques, and technologies.



TACIT security focuses on the *organizational* aspects of cyber security...that is, how to effectively use the security tools, techniques, and technologies to achieve desired solutions.

TACIT security addresses institutional and cultural issues that help organizations
“Build It Right”



A night-time photograph of the Golden Gate Bridge, illuminated with warm orange lights. The bridge spans across a dark body of water, with city lights visible in the background. The sky is dark, and the bridge's structure is clearly visible against the night.

For bridge builders, it's all about physics—

Equilibrium, static and dynamic loads, vibrations, and resonance.



For information system developers, it's all about mathematics, computer science, architecture, and systems engineering—

Trustworthiness, assurance, penetration resistance and resilience.

*The national imperative for building stronger,
more resilient information systems...*

Software assurance.
Systems and security engineering.
Supply chain risk management.



- The security controls in NIST SP 800-53, Revision 4, move beyond good cyber security hygiene and continuous monitoring... into the space of ***system resiliency*** and strengthening the IT infrastructure to achieve that resiliency.



*Does your
information system
have 9 lives?*



Security should be a by-product
of good design and development
practices.

TACIT Security

- Threat
- Assets
- Complexity
- Integration
- Trustworthiness

MERRIAM-WEBSTER DICTIONARY

tac·it *adjective*

: expressed or understood
without being directly stated

Threat

- Develop a better understanding of the *modern threat space*, including the capability of adversaries to launch sophisticated, targeted cyber-attacks that exploit specific organizational vulnerabilities.
 - Clear key organizational personnel at Top Secret and/or TS SCI levels for access to classified threat data.
 - Include external and insider threat assessments.

Assets

- Conduct a comprehensive criticality analysis of *organizational assets* including information and information systems.
 - Use FIPS Publication 199 for mission/business impact analysis (triage).
 - Subdivide high, moderate, and low impact levels to provide greater fidelity on risk assessments.

Complexity

- Reduce the *complexity* of the information technology infrastructure including IT component products and information systems.
 - Use enterprise architecture to consolidate, optimize, and standardize the IT infrastructure.
 - Employ cloud computing architectures to reduce the number of IT assets that need to be managed.

Integration

- Integrate information security requirements and the security expertise of individuals into organizational *development* and *management processes*.
 - Embed security personnel into enterprise architecture, systems engineering, SDLC, and acquisition processes.
 - Coordinate security requirements with mission/business owners; become key stakeholders.

Trustworthiness

- Invest in more *trustworthy* and *resilient* information systems supporting organizational missions and business functions.
 - Isolate critical assets into separate enclaves.
 - Implement solutions with greater strength of mechanism.
 - Increase developmental and evaluation assurance.
 - Use modular design, layered defenses, component isolation.

Summary – TACIT Security

- Understand the cyber threat space.
- Conduct a thorough criticality analysis of organizational assets.
- Reduce complexity of IT infrastructure.
- Integrate security requirements into organizational processes.
- Invest in trustworthiness and resilience of IT components and systems.



Concepts supporting TACIT.

Dual Protection Strategies

Sometimes your information systems will be compromised even when you do everything right...

- **Boundary Protection**

Primary Consideration: *Penetration resistance.*

Adversary Location: *Outside defensive perimeter.*

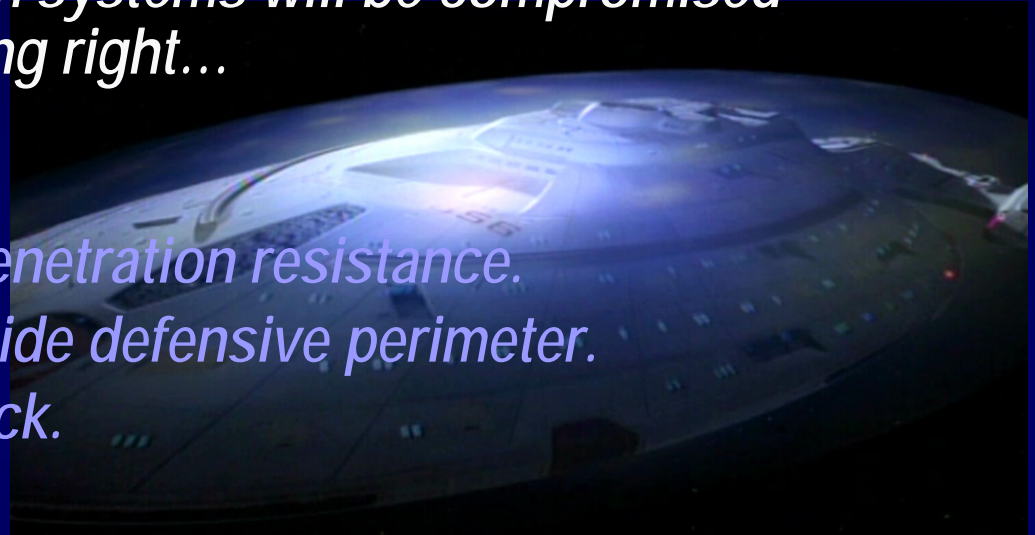
Objective: *Repel the attack.*

- **Agile Defense**

Primary Consideration: *Information system resilience.*

Adversary Location: *Inside defensive perimeter.*

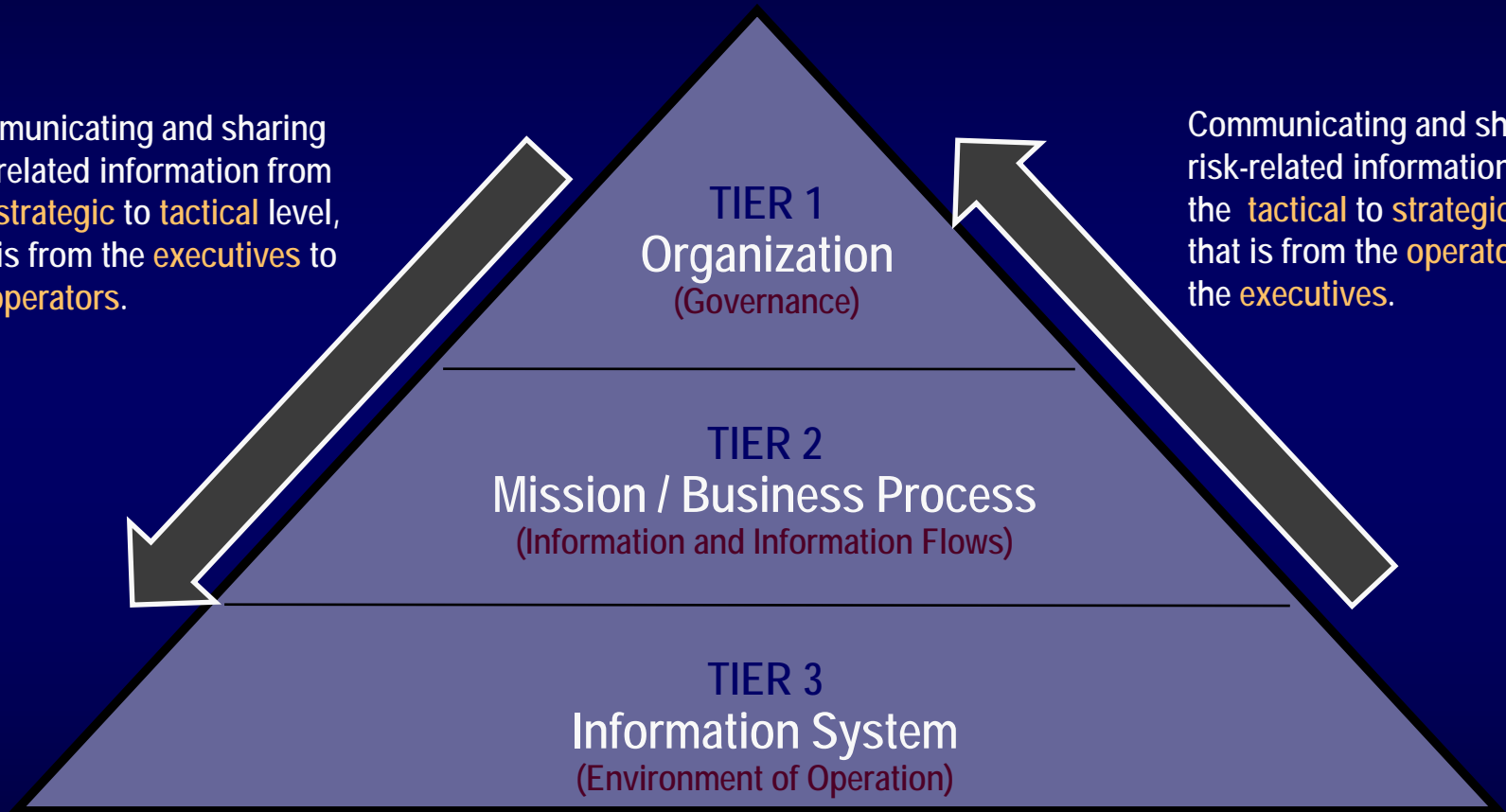
Objective: *Operate while under attack, limit damage, survive.*



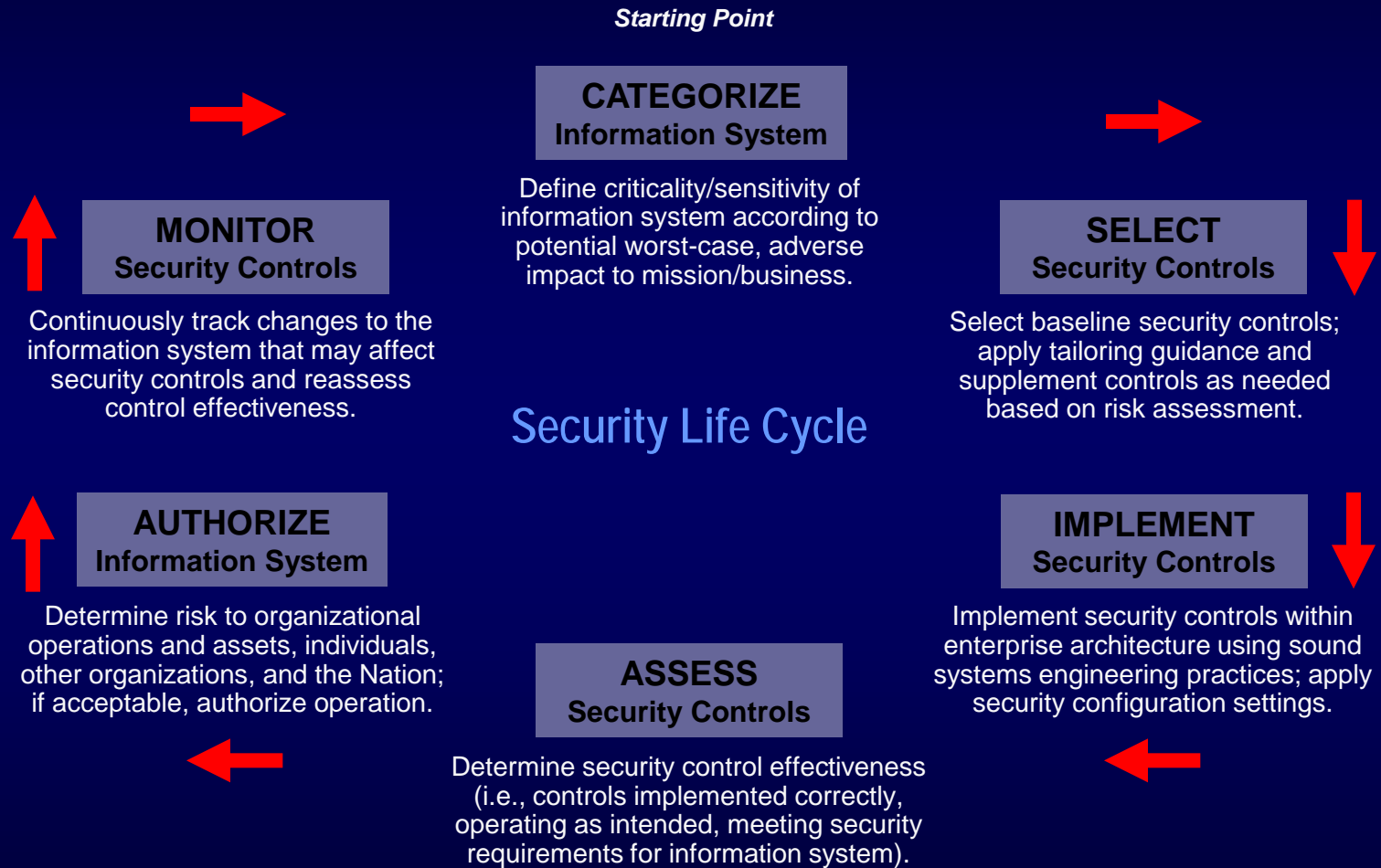
Institutionalizing Risk-Based Security

Communicating and sharing risk-related information from the **strategic** to **tactical** level, that is from the **executives** to the **operators**.

Communicating and sharing risk-related information from the **tactical** to **strategic** level, that is from the **operators** to the **executives**.



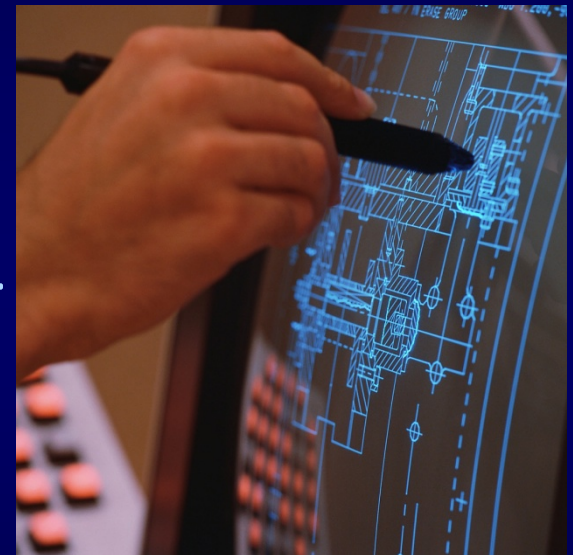
RMF Support – TACIT Security



Strengthening Specification Language

- Significant changes to security controls and control enhancements in—
 - Configuration Management family.
 - System and Services Acquisition family.
 - System and Information Integrity family.

Applying best practices in software development at all stages in the SDLC.



Platform Integrity

- *Investments in highly-assured trust technologies to establish the foundation for effective security including for example—*
 - Trusted Platform Module (hardware root of trust).
 - Protected BIOS (digitally-signed firmware).
 - Network Admissions Control (interaction between trusted platforms).



KEY CONCEPTS: secure generation of cryptographic keys (endorsement keys), memory curtaining/protected execution, sealed storage, remote attestation, and Trusted Third Party.

Key Publications – Built It Right

- NIST Special Publication 800-53, Revision 4
Security and Privacy Controls for Federal Information Systems and Organizations

April 2013



- NIST Special Publication 800-161
Supply Chain Risk Management Guideline

Initial Public Draft – August 2013



- NIST Special Publication 800-160
Security Engineering Guideline

Initial Public Draft – Spring 2014



Significant Updates to Security Controls

- Development processes, standards, and tools.
- Developer security architecture and design.
- Developer configuration management.
- Developer security testing.
- Developer-provided training.
- Supply chain protection.



Build It Right – Continuously Monitor


- State-of-the-practice security and privacy controls to protect federal missions and business functions.
- Overlays tailored to missions/business functions, environments of operation, and technologies.
- Greater situational awareness from continuous monitoring.

Some final thoughts.



We choose to go to the moon in this decade and do other things. Not because they are easy, but because they are hard.

-- John F. Kennedy, 1961



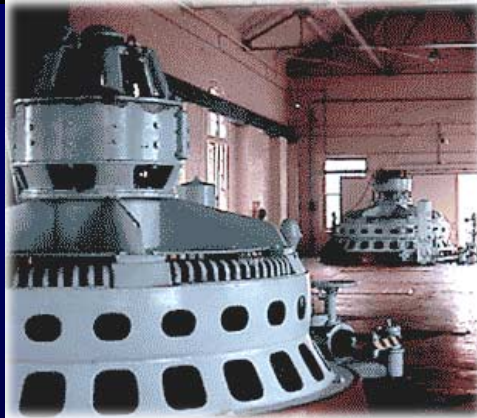
Cybersecurity is the great challenge
of the 21st century.

Cybersecurity problems are hard—
not easy.

Are we prepared to do the heavy lifting?



Critical assets must be protected differently than non-critical assets.



Critical organizational missions and business functions are at risk...



Be *proactive*, not *reactive* when it comes to protecting your organizational assets.

Necessary *and* Sufficient Security Solutions...



**Cyber Security
Hygiene**

*COUNTING, CONFIGURING,
AND PATCHING IT ASSETS*



**Strengthening
the IT Infrastructure**

*SYSTEM/SECURITY ENGINEERING,
ARCHITECTURE, AND RESILIENCY*

Has your organization achieved the appropriate balance?

The clock is ticking—
the time to act is now.



*Failure is not an option...
when freedom and economic
prosperity are at stake.*





Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Project Leader

Dr. Ron Ross
(301) 975-5390
ron.ross@nist.gov

Administrative Support

Peggy Himes
(301) 975-2489
peggy.himes@nist.gov

Senior Information Security Researchers and Technical Support

Pat Toth
(301) 975-5140
patricia.toth@nist.gov

Kelley Dempsey
(301) 975-2827
kelley.dempsey@nist.gov

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Web: csrc.nist.gov/sec-cert

Comments: sec-cert@nist.gov