Convener’s Remarks, Meeting #1 of ISO/IEC JTC 1/SC 22/OWG:V

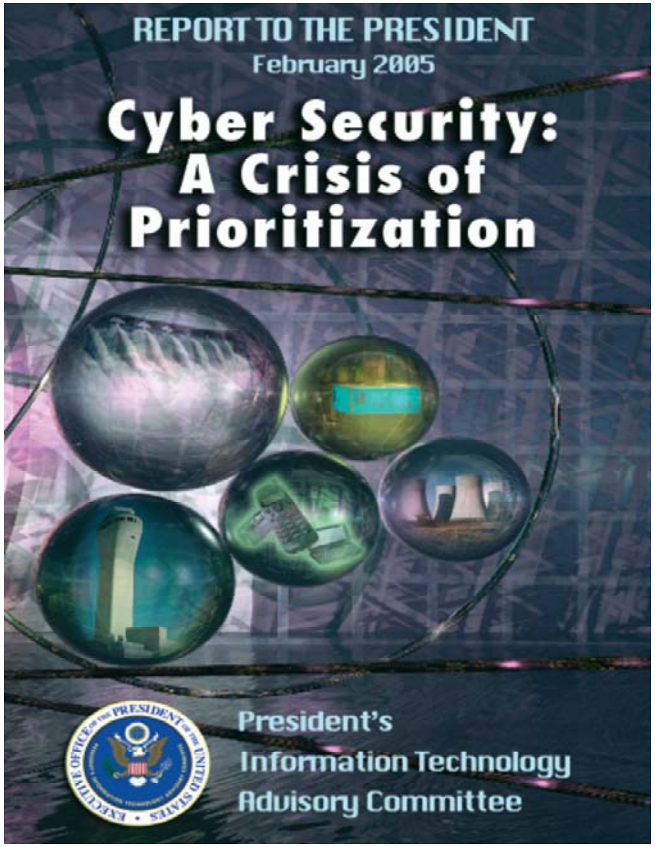
Jim Moore
Convener, ISO/IEC JTC 1/SC 22/OWG Vulnerability
James.W.Moore@ieee.org

Cyber Security is a Growing Problem

President’s Information Technology Advisory Committee (PITAC) Subcommittee on Cyber Security

Areas in Need of Increased Support

- Computer Authentication Methodologies
- Securing Fundamental Protocols
- ***Secure Software Engineering and Software Assurance***
- Holistic System Security
- Monitoring and Detection
- Mitigation and Recovery Methodologies
- Cyber Forensics and Technology to Enable Prosecution of Criminals
- Modeling and Testbeds for New Technologies
- Metrics, Benchmarks, and Best Practices
- Societal and Governance Issues



REPORT TO THE PRESIDENT

February 2005

Cyber Security: A Crisis of Prioritization

President’s Information Technology Advisory Committee

-- From Joe Jarzombek, PMP, Director for Software Assurance, NCSD, DHS

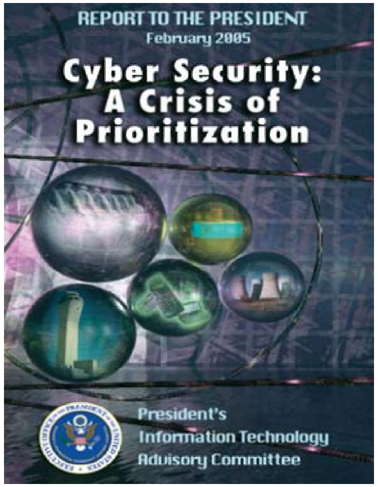
Threat

The problem has implications for:

- **Safety**
- **Privacy**
- **Security**
- **Economy**
- **Even national security**

-- From Joe Jarzombek, PMP, Director for Software Assurance, NCSD, DHS

PITAC's Findings Relative to Needs for Secure Software Engineering & Software Assurance


REPORT TO THE PRESIDENT
February 2005
Cyber Security: A Crisis of Prioritization
President's Information Technology Advisory Committee

- Commercial software engineering today lacks the scientific underpinnings and rigorous controls needed to produce high-quality, secure products at acceptable cost.
- Commonly used software engineering practices permit dangerous errors, such as improper handling of buffer overflows, which enable hundreds of attack programs to compromise millions of computers every year.
- In the future, the Nation may face even more challenging problems as adversaries – both foreign and domestic – become increasingly sophisticated in their ability to insert malicious code into critical software.

Government Response

There are initiatives underway in the US, in both Defense and Homeland Security.

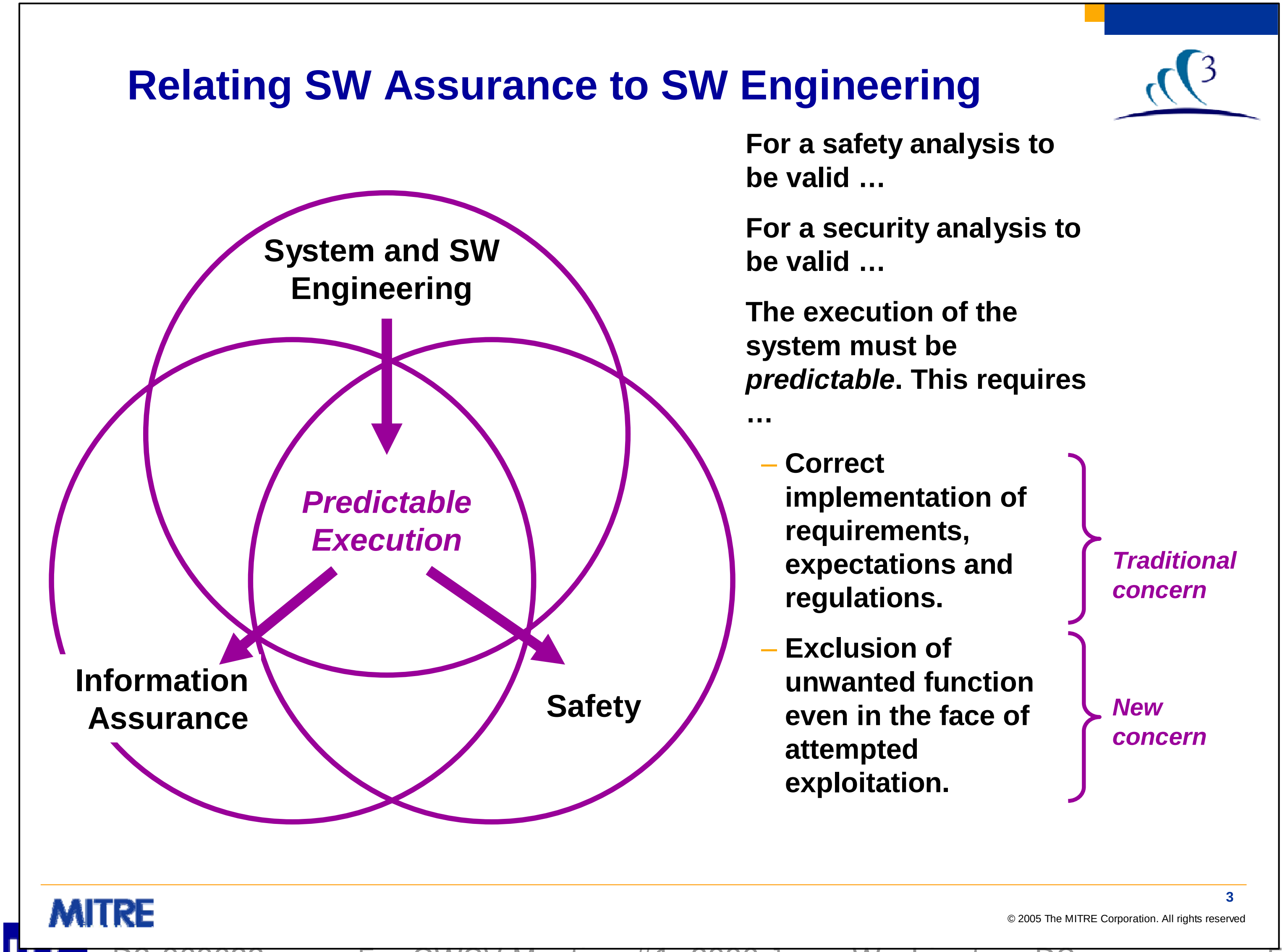
-- From Joe Jarzombek, PMP, Director for Software Assurance, NCSD, DHS

DHS Software Assurance Initiative

- **Purpose**:
  - Shift security paradigm from Patch Management to Software Assurance
  - Encourage the software developers (public and private industry) to raise the bar on software quality and security
  - Facilitate discussion, develop practical guidance, review tools, and promote R&D investment
- **Charter -- The National Strategy to Secure Cyberspace - Action/Recommendation 2-14:**

"DHS will facilitate a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development."

Relationship of Software Assurance to Other Disciplines


System and SW Engineering
Predictable Execution
Information Assurance
Safety

Relating SW Assurance to SW Engineering

For a safety analysis to be valid …

For a security analysis to be valid …

The execution of the system must be ***predictable***. This requires …

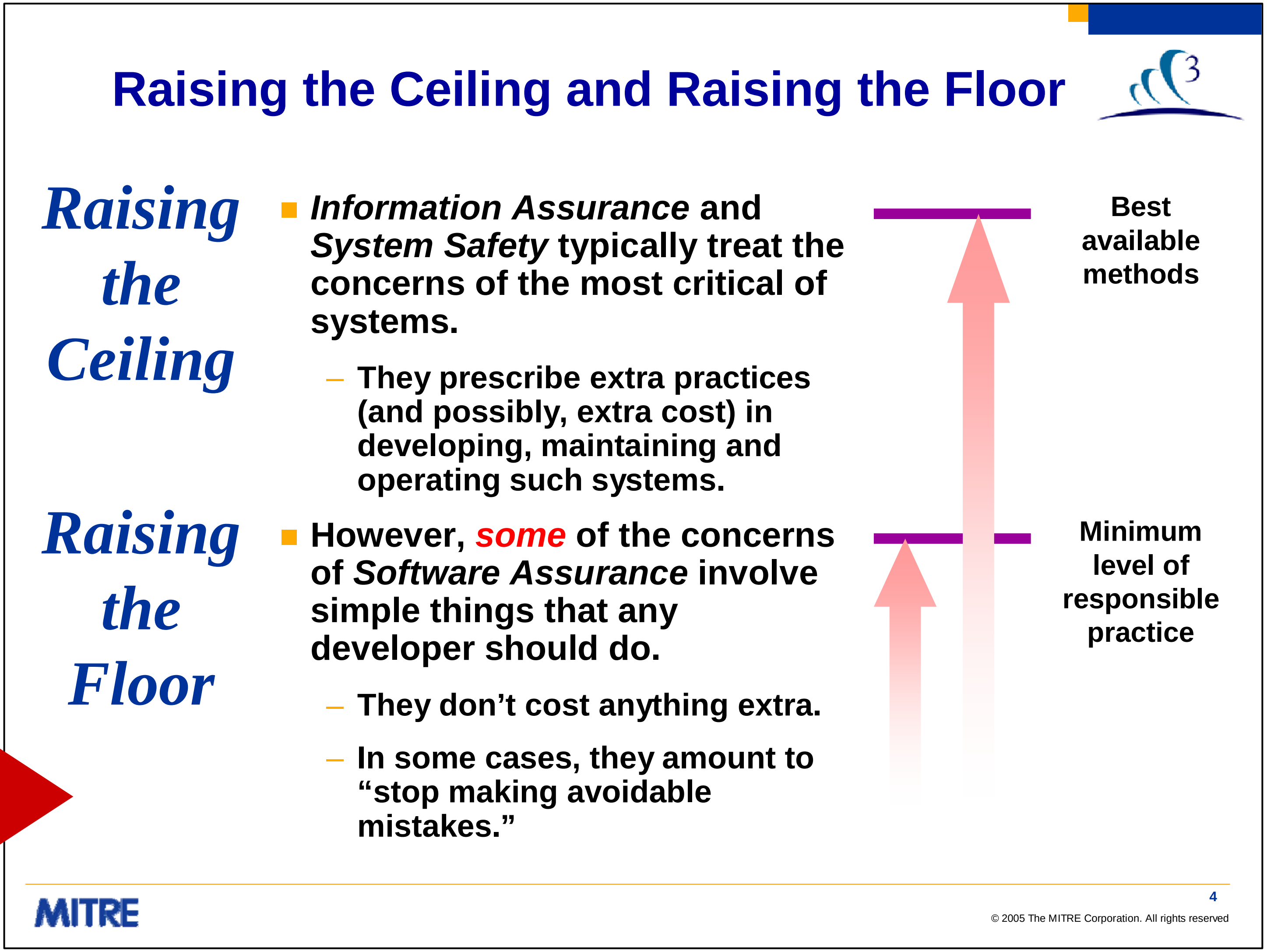
- Correct implementation of requirements, expectations and regulations.
- Exclusion of unwanted function even in the face of attempted exploitation.

Traditional concern

New concern

Relationship of Software Assurance to Other Disciplines

Some "avoidable mistakes" are encouraged by poor usage (arguably, poor design) of programming languages.



Raising the Ceiling and Raising the Floor

Raising the Ceiling

- ***Information Assurance*** **and** ***System Safety*** **typically treat the concerns of the most critical of systems.**
  - **They prescribe extra practices (and possibly, extra cost) in developing, maintaining and operating such systems.**

Raising the Floor

- **However, *some* of the concerns of *Software Assurance* involve simple things that any developer should do.**
  - **They don't cost anything extra.**
  - **In some cases, they amount to "stop making avoidable mistakes."**

MITRE

4

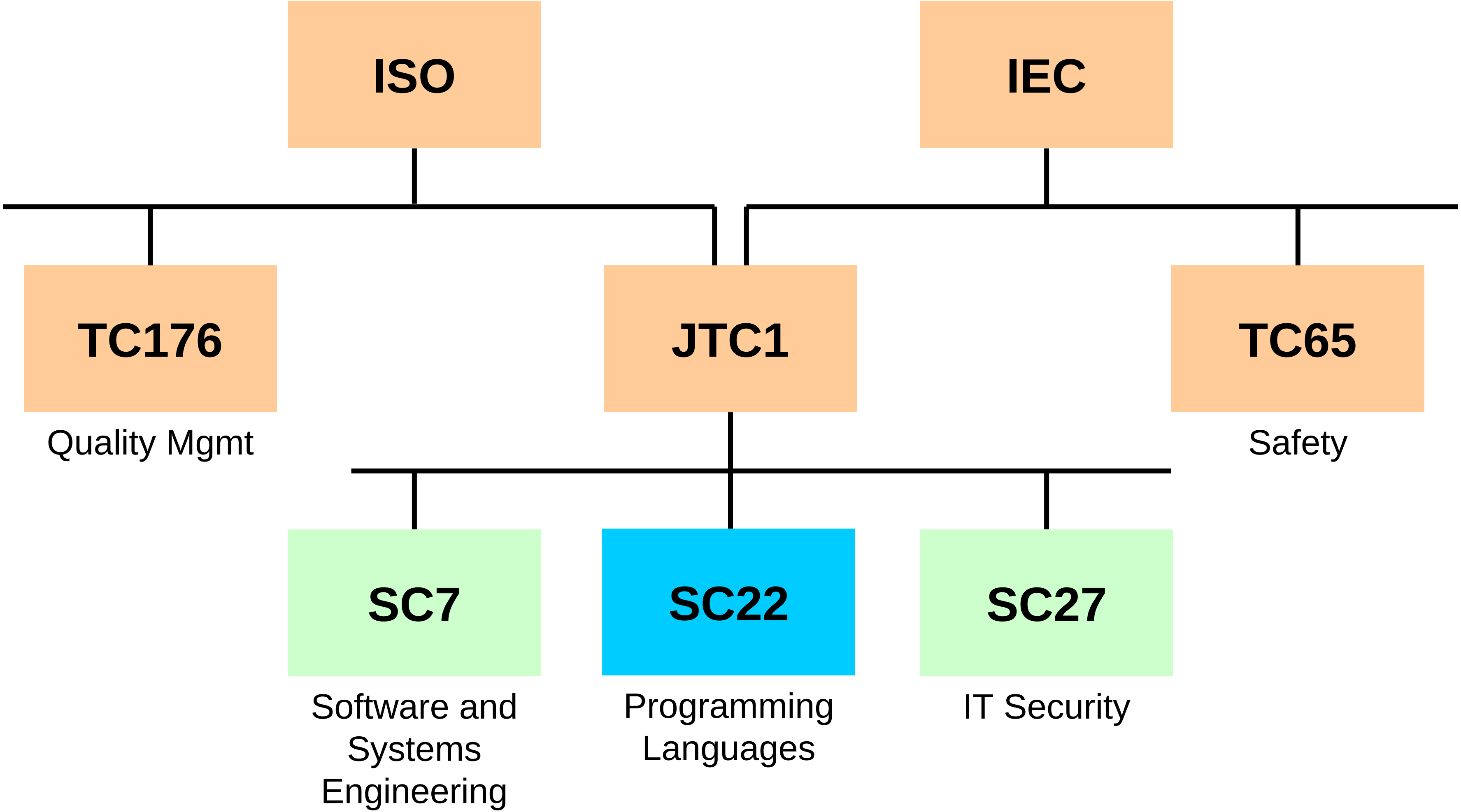
Problem

- Any programming language has constructs that are imperfectly defined, implementation-dependent or difficult to use correctly.
- As a result, software programs sometimes execute differently than intended by the writer.
- In some cases, these vulnerabilities can be exploited by unfriendly parties.
  - Can compromise safety, security and privacy.
  - Can be used to make additional attacks.

Complicating Factors

- The choice of programming language for a project is not solely a technical decision and is not made solely by software engineers.
- Some vulnerabilities cannot be mitigated by better use of the language but require mitigation by other methods, e.g. review, static analysis.

Relevant International Standards Committees



Officers

- John Hill, Chair, ISO/IEC JTC 1/SC 22
- Sally Seitz (ANSI), Secretariat, SC 22
- Jim Moore, Convener, SC 22/OWGV
- John Benito, Co-Convener, SC 22/OWGV
- Secretary ?
- Project Editor ?

John Hill: John.Hill@sun.com
Sally Seitz: sseitz@ansi.org
Jim Moore: James.W.Moore@ieee.org
John Benito: jb@benito.com

Participation

Participant	NB Delegate	WG Liaison	Other Liaison
John Benito	US	WG14 (C)	
Ben Brosgol			RT/SC Java
Rod Chapman			SPARK
Franco Gasperoni	France (HOD)		
Cesar Gonzalez-Perez			SC 7/WG 19
Barry Hedquist	US		
Kiyoshi Ishihata	Japan (HOD)		
Rex Jaeschke	US (HOD)		
Derek Jones	UK (HOD)		
Stephen Michell	Canada (HOD)		
Ed de Moel	US		MDC (MUMPS)
Jim Moore	US		
Dan Nagle	US	?	J3 (Fortran)
Erhard Ploedereder	Germany (HOD)	WG9 (Ada)	
Tom Plum	US	?	ECMA TC39/TG2 (C#)
Robert Seacord			CERT
Barry Tauber		?	J4 (Cobol)

Progress

2005-10	SC 22 approves NP for project 24772.
2005-10	SC 22 creates OWGV; Moore is appointed as convener.
2005-11	Moore makes information briefing to WG9.
2005-03	Benito named as co-convener of OWGV.
2005-03	Moore makes information briefing to WG14. Benito briefs WG21.
2005-03	Disposition of comments on NP filed.
2006-06	Benito makes information briefing to WG9.
2006-06	OWGV Meeting #1, 26-27 June, Washington, DC
2006-09	OWGV Meeting #2, 14-15 September, London, UK