Information Security: The Legacy of a Maginot Line in Cyberspace

Doug DePeppe
Founder, i2IS

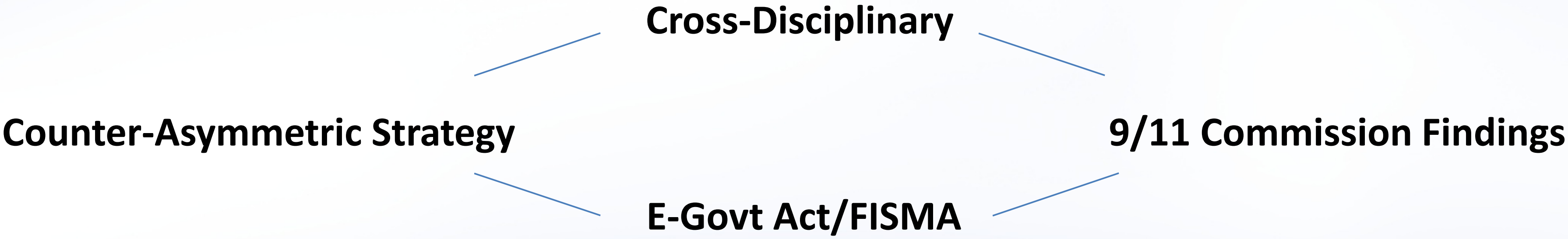
doug.depeppe@i2iscorp.com
719-785-0355

Information Security: The Legacy of a Maginot Line in Cyberspace

Theme:

Today’s Sophisticated Cyberspace Threat Environment Necessitates A New, Cross-Disciplinary Approach to Cybersecurity

Today's Sophisticated Cyberspace Threat Environment Necessitates A New, Cross-Disciplinary Approach to Cybersecurity



Cross-Disciplinary

Counter-Asymmetric Strategy

9/11 Commission Findings

E-Govt Act/FISMA

DISCIPLINARY CONSTRUCT

EXPLORING THE CONTOURS OF THE PROBLEM

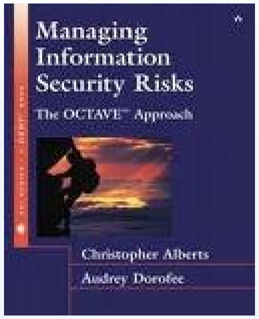
CNSSI 1253 ➡ DOD DIACAP, eff Nov 2007

⬇

DOD DIARMF (SP 800-37/53)

COBIT®
GOVERNANCE, CONTROL and AUDIT for INFORMATION and RELATED TECHNOLOGY

“<u>Standards Soup</u>”


Managing Information Security Risks
The OCTAVE™ Approach
Christopher Alberts
Audrey Dorofee

ISO International Organization for Standardization

National Institute of Standards and Technology

NIST National Institute of Standards and Technology

EXPLORING THE CONTOURS OF THE PROBLEM

Expense and duration of ISO 27001/27002 implementation

$40,000
$100,000
$200,000
$500,000

Duration: several months years

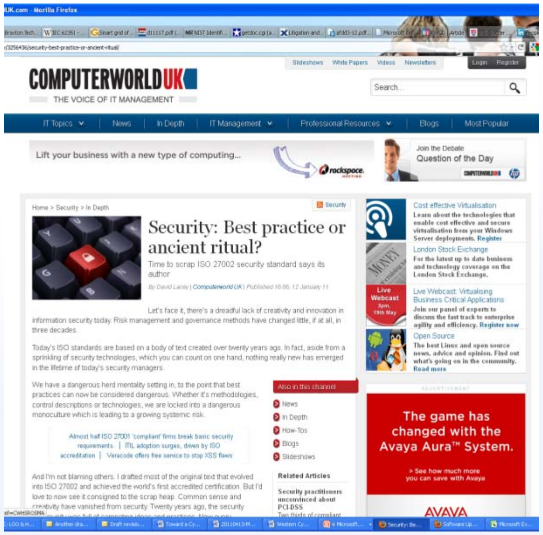
Vulnerability and Pen Tests: $100's to $1000's Good Enough?

What is the Goal?

What is Cybersecurity?

COMPUTERWORLDUK

THE VOICE OF IT MANAGEMENT



Security: Best practice or ancient ritual?

Time to scrap ISO 27002 security standard says its author

By David Lacey | Computerworld UK | Published 16:06, 12 January 11

Let's face it, there's a dreadful lack of creativity and innovation in information security today. Risk management and governance methods have changed little, if at all, in three decades.

Today's ISO standards are based on a body of text created over twenty years ago. In fact, aside from a sprinkling of security technologies, which you can count on one hand, nothing really new has emerged in the lifetime of today's security managers.

We have a dangerous herd mentality setting in, to the point that best practices can now be considered dangerous. Whether it's methodologies, control descriptions or technologies, we are locked into a dangerous monoculture which is leading to a growing systemic risk.

Almost half ISO 27001 'compliant' firms break basic security requirements | ITIL adoption surges, driven by ISO accreditation | Veracode offers free service to stop XSS flaws

And I'm not blaming others. I drafted most of the original text that evolved into ISO 27002 and achieved the world's first accredited certification. But I'd love to now see it consigned to the scrap heap. Common sense and creativity have vanished from security. Twenty years ago, the security

Security practitioners unconvinced about PCI-DSS

Two thirds of compliant

Cost effective Virtualisation

Learn about the technologies that enable cost effective and secure virtualisation from your Windows Server deployments. Register

London Stock Exchange

For the latest up to date business and technology coverage on the London Stock Exchange.

Live Webcast: Virtualising Business Critical Applications

Join our panel of experts to discuss the fast track to enterprise agility and efficiency. Register now

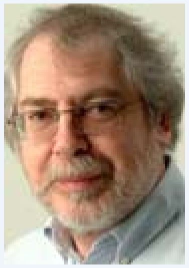
Open Source

The best Linux and open source news, advice and opinion. Find out what's going on in the community. Read more

Mr. David Lacey, ISO 27002 author:

Today's ISO standards are based on a body of text created over twenty years ago. In fact, aside from a sprinkling of security technologies, which you can count on one hand, nothing really new has emerged in the lifetime of today's security managers.

Security managers are chained to a <u>backward-looking compliance treadmill</u> that gives priority to <u>old legacy practices</u>, paperwork that no one reads, and outstanding audit actions from previous years.



"I'd love to now see it consigned to the scrap heap."

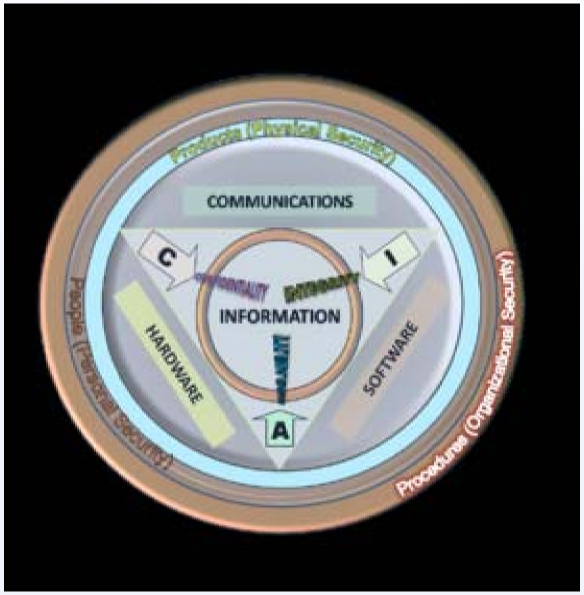
EXPLORING THE CONTOURS OF THE PROBLEM

Contour One:

Controls-based approach

Problematic Aspects:

- **Static**
- **Compliance mindset**
- **Interoperability**
- **Discoverable model for attackers**


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
HARDWARE
SOFTWARE
A
People (Personal Security)
Procedures (Organizational Security)

C - I - A

EXPLORING THE CONTOURS OF THE PROBLEM

Some people think technology has the answers.
Kevin Mitnick

My message today is primarily the same... I usually go around speaking on the threat of the human element, particularly on social engineering.
Kevin Mitnick

Peer-to-Peer

Zero Day Exploits

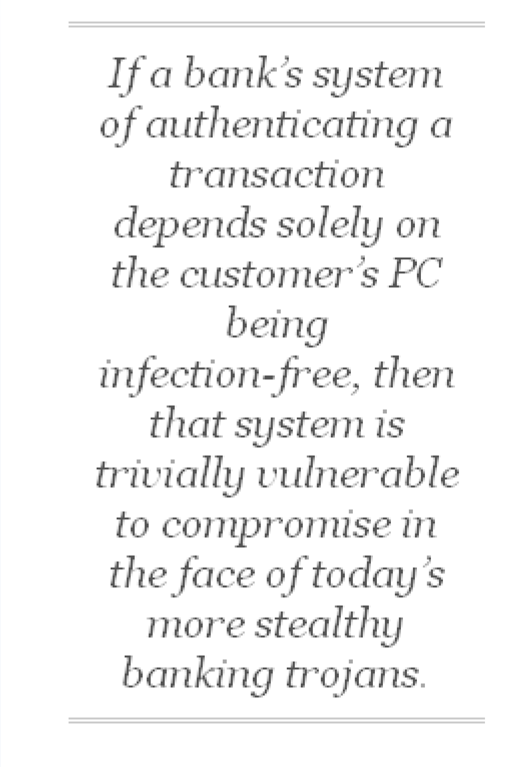
Mobile Media Devices

Advanced Persistent Threat

KrebsonSecurity

In-depth security news and investigation

Commingling data & Devices between Trusted & Untrusted Domains



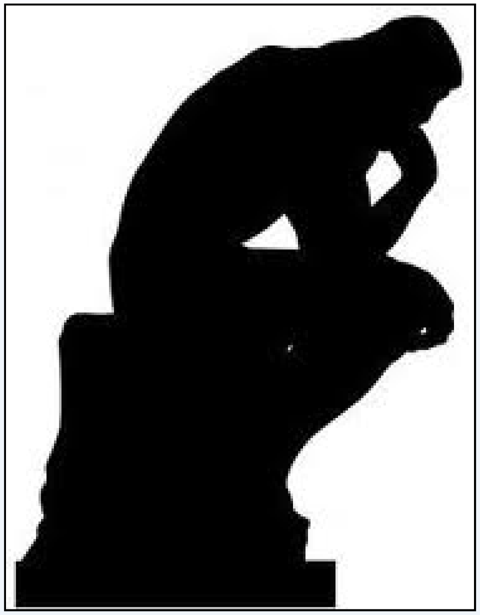
If a bank's system of authenticating a transaction depends solely on the customer's PC being infection-free, then that system is trivially vulnerable to compromise in the face of today's more stealthy banking trojans.

Zeus
Botnets
Social Networks

The Internet Today

EXPLORING THE CONTOURS OF THE PROBLEM

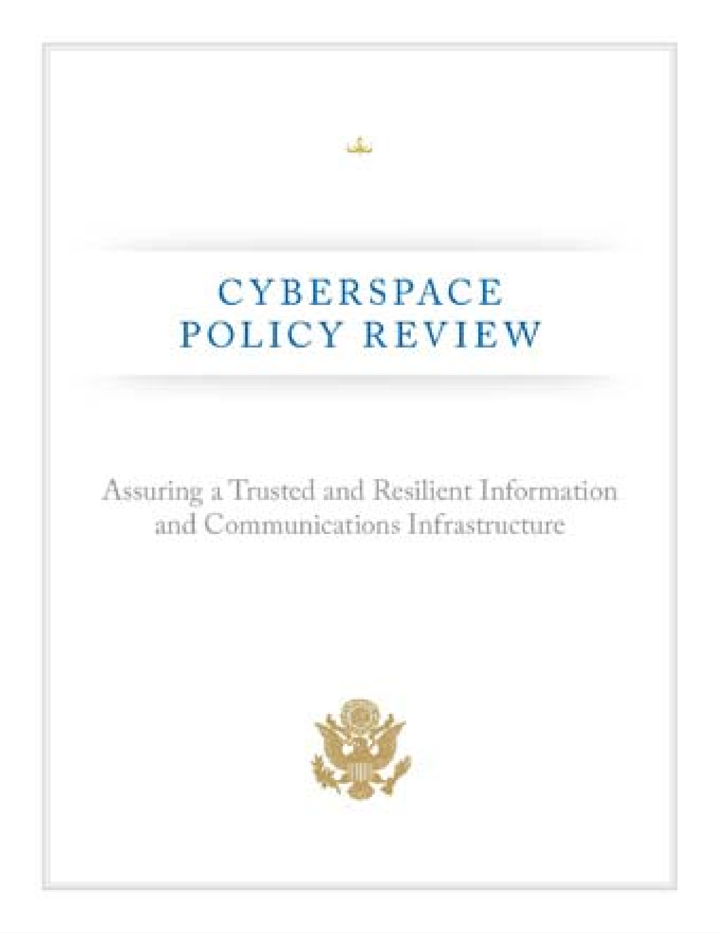
Contour Two:
Problem-solving



<u>Problematic Aspects:</u>

- **Proper problem identification**
- **Scope**
- **Empowerment for security**
  - **organizational**
  - **macro driving a market**
- **Leadership**

What is Cybersecurity?



CYBERSPACE POLICY REVIEW

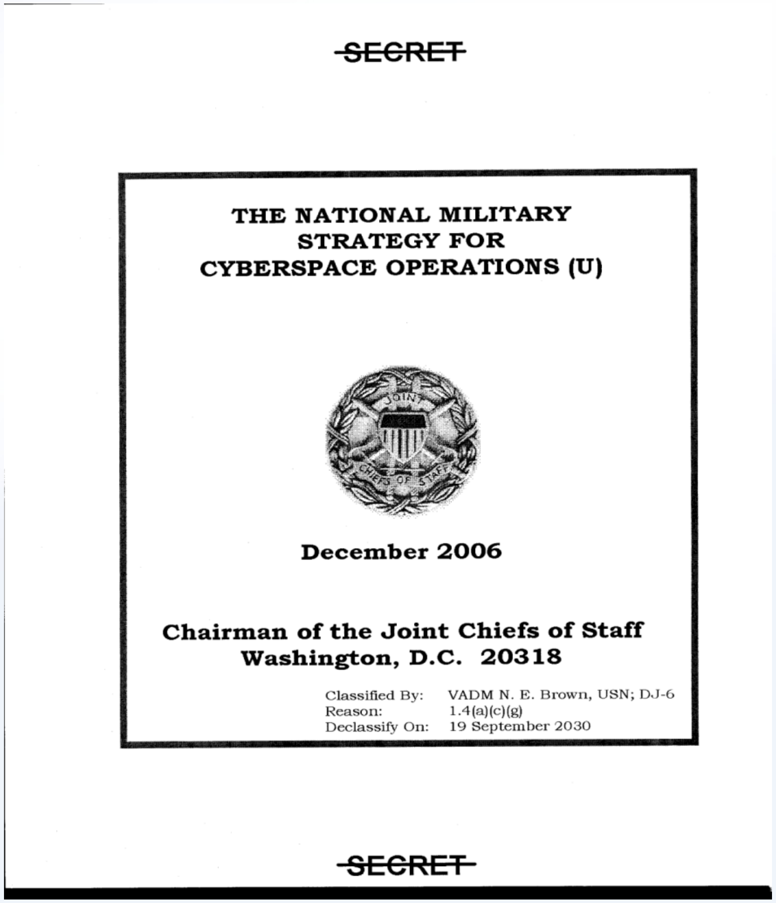
Assuring a Trusted and Resilient Information and Communications Infrastructure

THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003

What is Cybersecurity?



~~SECRET~~

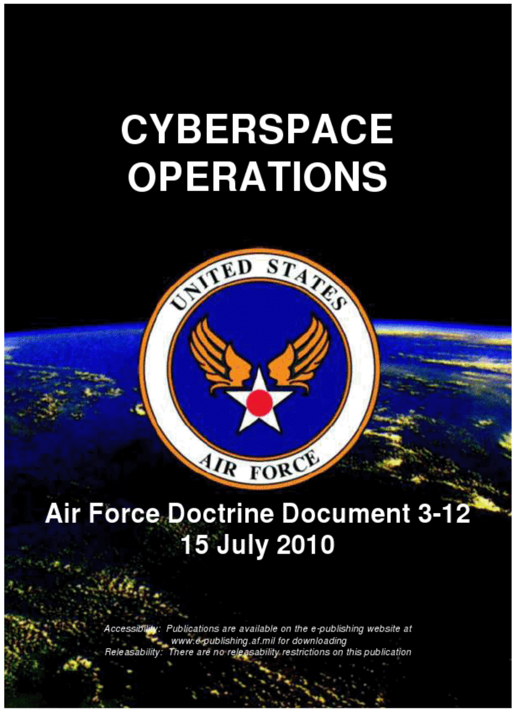
THE NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS (U)

December 2006

Chairman of the Joint Chiefs of Staff
Washington, D.C. 20318

Classified By:	VADM N. E. Brown, USN; DJ-6
Reason:	1.4(a)(c)(g)
Declassify On:	19 September 2030

~~SECRET~~



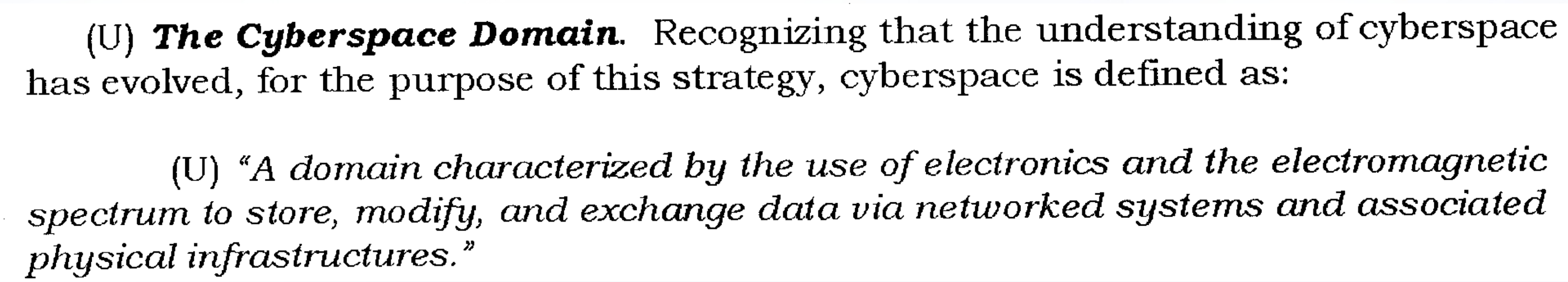
CYBERSPACE OPERATIONS

Air Force Doctrine Document 3-12
15 July 2010

Accessibility: Publications are available on the e-publishing website at www.e-publishing.af.mil for downloading
Releasability: There are no releasability restrictions on this publication

EXPLORING THE CONTOURS OF THE PROBLEM

National Military Strategy



(U) ***The Cyberspace Domain***. Recognizing that the understanding of cyberspace has evolved, for the purpose of this strategy, cyberspace is defined as:

> (U) *"A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures."*

Joint Publication (JP) 1-02,
Department of Defense Dictionary of Military and Associated Terms

Cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

EXPLORING THE CONTOURS OF THE PROBLEM

Securing Cyberspace versus defining Cybersecurity?

Cyberspace is “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”

Cybersecurity and Internet Freedom Act of 2011 S. 413

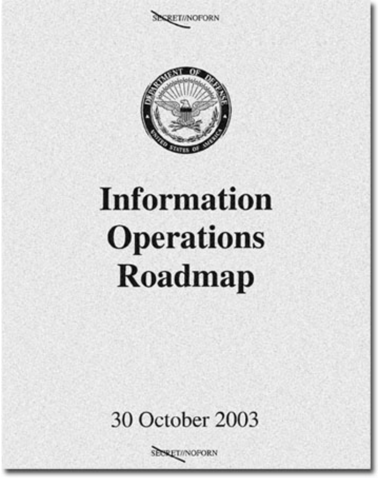
NATIONAL STRATEGY.—The term ''National Strategy'' means the national strategy to increase the security and resiliency of cyberspace developed under section 101(a)(1).

Sec 101. There is established in the Executive Office of the President an Office of Cyberspace Policy which shall—

Develop … a national strategy to increase the security and resiliency of cyberspace [including]:

- Computer network operations
- information assurance
- critical infrastructure
- R&D priorities
- law enforcement
- diplomacy
- homeland security
- privacy & civil liberties
- intelligence activities
- identify management/authentication

EXPLORING THE CONTOURS OF THE PROBLEM

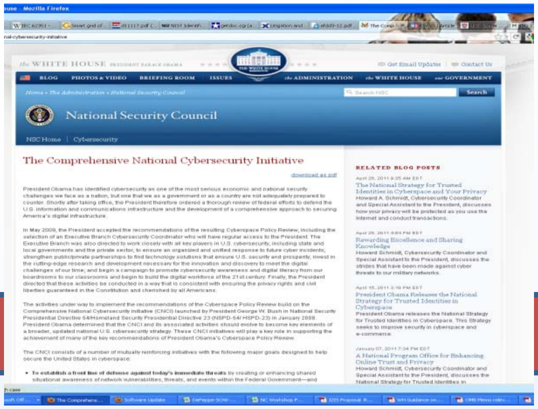

~~SECRET~~//NOFORN

Information Operations Roadmap

30 October 2003

~~SECRET~~//NOFORN

2003



National Security Council

The Comprehensive National Cybersecurity Initiative

President Obama has identified cybersecurity as one of the most serious economic and national security challenges we face as a nation, but one that we as a government or as a country are not adequately prepared to counter. Shortly after taking office, the President therefore ordered a thorough review of federal efforts to defend the U.S. information and communications infrastructure and the development of a comprehensive approach to securing America's digital infrastructure.

In May 2009, the President accepted the recommendations of the resulting Cyberspace Policy Review, including the selection of an Executive Branch Cybersecurity Coordinator who will have regular access to the President. The Executive Branch was also directed to work closely with all key players in U.S. cybersecurity, including state and local governments and the private sector, to ensure an organized and unified response to future cyber incidents; strengthen public/private partnerships to find technology solutions that ensure U.S. security and prosperity; invest in the cutting-edge research and development necessary for the innovation and discovery to meet the digital challenges of our time; and begin a campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and begin to build the digital workforce of the 21st century. Finally, the President directed that these activities be conducted in a way that is consistent with ensuring the privacy rights and civil liberties guaranteed in the Constitution and cherished by all Americans.

The activities under way to implement the recommendations of the Cyberspace Policy Review build on the Comprehensive National Cybersecurity Initiative (CNCI) launched by President George W. Bush in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) in January 2008. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy. These CNCI initiatives will play a key role in supporting the achievement of many of the key recommendations of President Obama's Cyberspace Policy Review.

The CNCI consists of a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace:

- **To establish a front line of defense against today's immediate threats** by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and

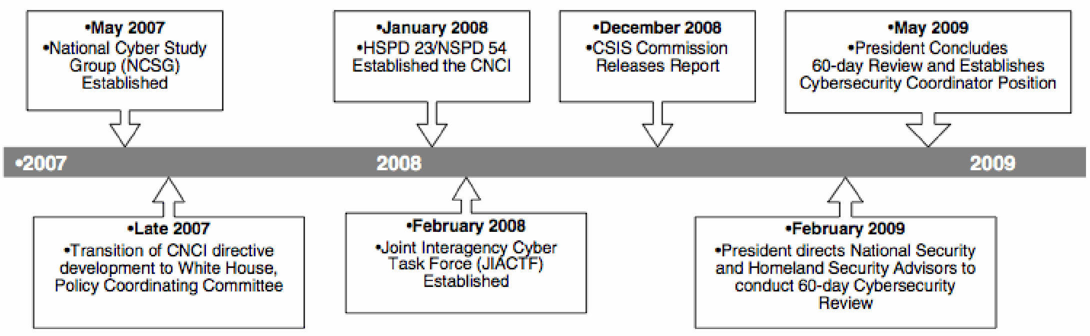
RELATED BLOG POSTS

April 26, 2011 9:35 AM EDT
The National Strategy for Trusted Identities in Cyberspace and Your Privacy
Howard A. Schmidt, Cybersecurity Coordinator and Special Assistant to the President, discusses how your privacy will be protected as you use the Internet and conduct transactions.

April 26, 2011 4:04 PM EDT
Rewarding Excellence and Sharing Knowledge
Howard Schmidt, Cybersecurity Coordinator and Special Assistant to the President, discusses the strides that have been made against cyber threats to our military networks.

April 15, 2011 3:19 PM EDT
President Obama Releases the National Strategy for Trusted Identities in Cyberspace
President Obama releases the National Strategy for Trusted Identities in Cyberspace. This Strategy seeks to improve security in cyberspace and e-commerce.

January 07, 2011 7:34 PM EST
A National Program Office for Enhancing Online Trust and Privacy
Howard Schmidt, Cybersecurity Coordinator and Special Assistant to the President, discusses the National Strategy for Trusted Identities in



•May 2007
•National Cyber Study Group (NCSG) Established

•Late 2007
•Transition of CNCI directive development to White House, Policy Coordinating Committee

•January 2008
•HSPD 23/NSPD 54 Established the CNCI

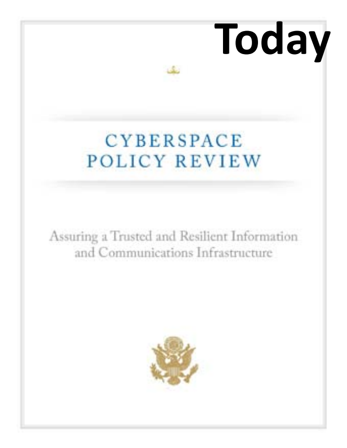
•February 2008
•Joint Interagency Cyber Task Force (JIACTF) Established

•December 2008
•CSIS Commission Releases Report

•February 2009
•President directs National Security and Homeland Security Advisors to conduct 60-day Cybersecurity Review

•May 2009
•President Concludes 60-day Review and Establishes Cybersecurity Coordinator Position

Today


CYBERSPACE POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure

Are We Making Gains?

EXPLORING THE CONTOURS OF THE PROBLEM

Contour Three:

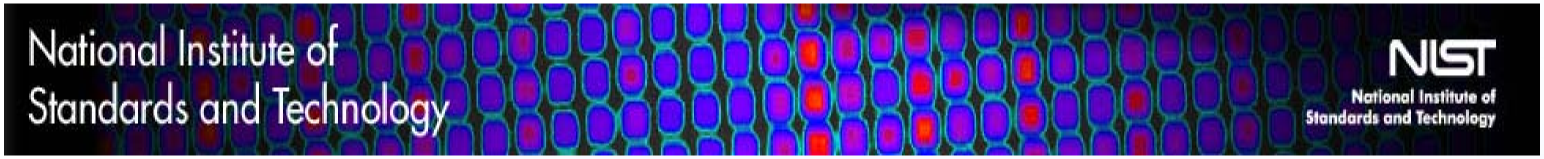
Leadership Lacking

Problematic Aspects

- **Lack of full understanding of**
  - **dynamics, and**
  - **components**
- **Lack of direction = risk = stalls initiative**
- **Legacy constructs persist/Stagnation**

EXPLORING THE CONTOURS OF THE PROBLEM

→ **Start Points Often Dictate End Points** ←

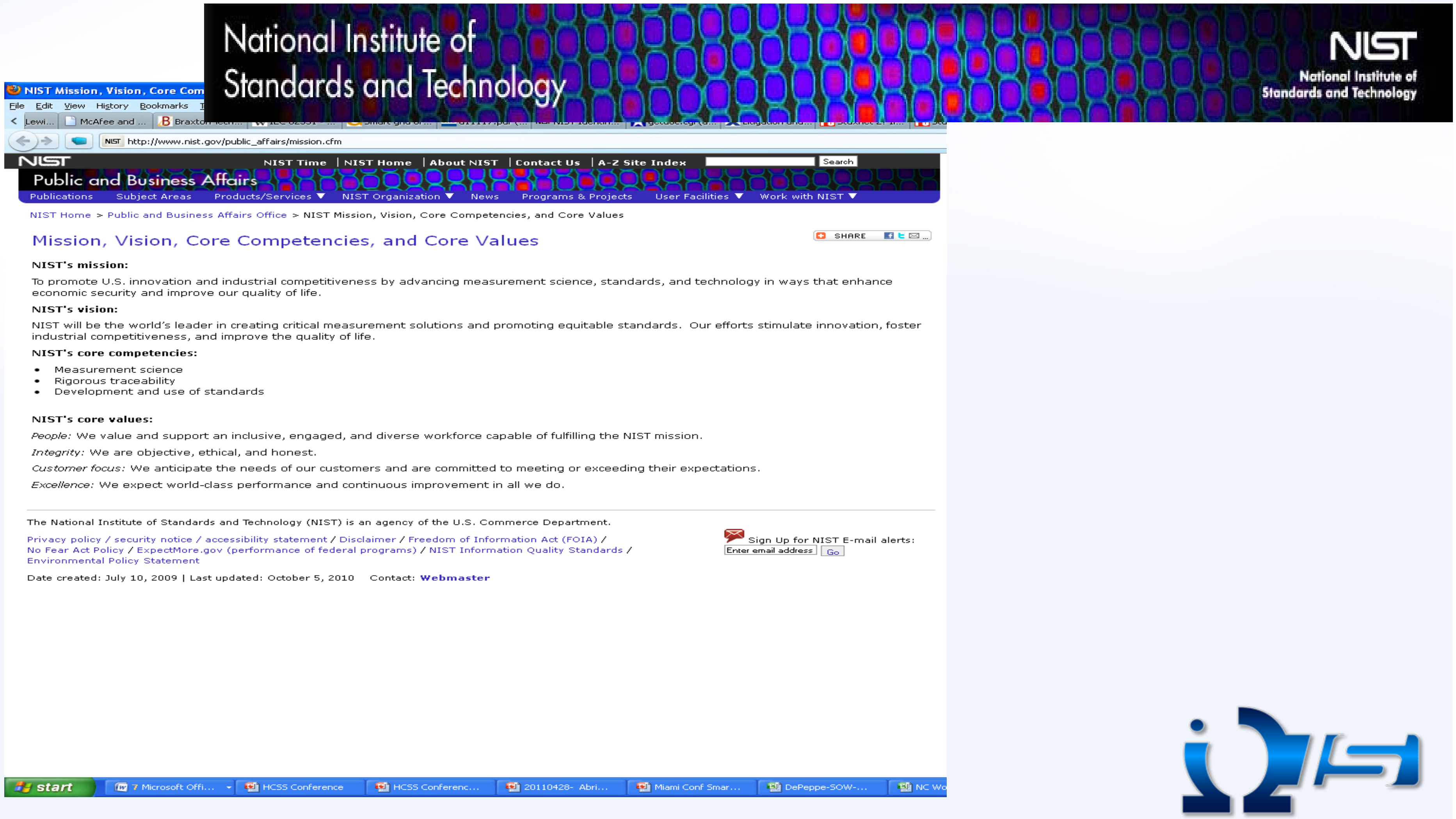


E-Government Act of 2002 (FISMA)

Defined "information security" as the goal –> standard C – I – A construct

Charged NIST with establishing "information security" standards

EXPLORING THE CONTOURS OF THE PROBLEM



National Institute of Standards and Technology
NIST
National Institute of Standards and Technology
NIST Mission, Vision, Core Com
File Edit View History Bookmarks
Lewi... McAfee and ... Braxton Tech...
http://www.nist.gov/public_affairs/mission.cfm
NIST
NIST Time | NIST Home | About NIST | Contact Us | A-Z Site Index
Search
Public and Business Affairs
Publications Subject Areas Products/Services NIST Organization News Programs & Projects User Facilities Work with NIST
SHARE
start
7 Microsoft Offi...
HCSS Conference
HCSS Conferenc...
20110428- Abri...
Miami Conf Smar...
DePeppe-SOW-...
NC Wo

NIST Home > Public and Business Affairs Office > NIST Mission, Vision, Core Competencies, and Core Values

Mission, Vision, Core Competencies, and Core Values

NIST's mission:

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST's vision:

NIST will be the world's leader in creating critical measurement solutions and promoting equitable standards. Our efforts stimulate innovation, foster industrial competitiveness, and improve the quality of life.

NIST's core competencies:

- Measurement science
- Rigorous traceability
- Development and use of standards

NIST's core values:

People: We value and support an inclusive, engaged, and diverse workforce capable of fulfilling the NIST mission.

Integrity: We are objective, ethical, and honest.

Customer focus: We anticipate the needs of our customers and are committed to meeting or exceeding their expectations.

Excellence: We expect world-class performance and continuous improvement in all we do.

The National Institute of Standards and Technology (NIST) is an agency of the U.S. Commerce Department.

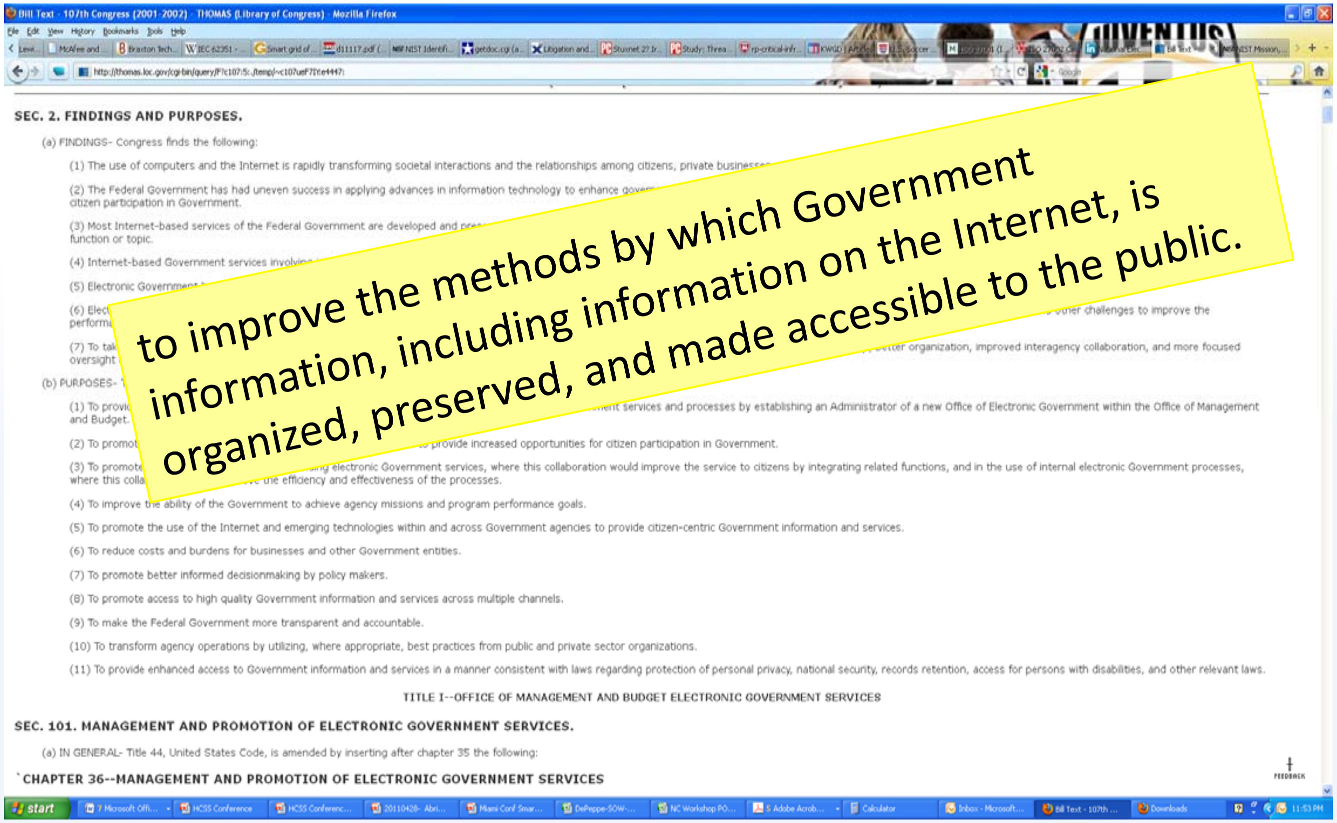
Privacy policy / security notice / accessibility statement / Disclaimer / Freedom of Information Act (FOIA) / No Fear Act Policy / ExpectMore.gov (performance of federal programs) / NIST Information Quality Standards / Environmental Policy Statement

Sign Up for NIST E-mail alerts: Enter email address Go

Date created: July 10, 2009 | Last updated: October 5, 2010 Contact: **Webmaster**

E-Government Act of 2002

No Mention of
information security


Bill Text - 107th Congress (2001-2002) - THOMAS (Library of Congress) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://thomas.loc.gov/cgi-bin/query/F?c107:5:./temp/~c107ueF7It:e4447:
start
11:53 PM
FEEDBACK

SEC. 2. FINDINGS AND PURPOSES.

(a) FINDINGS- Congress finds the following:

(1) The use of computers and the Internet is rapidly transforming societal interactions and the relationships among citizens, private businesses

(2) The Federal Government has had uneven success in applying advances in information technology to enhance gover
citizen participation in Government.

(3) Most Internet-based services of the Federal Government are developed and pres
function or topic.

(4) Internet-based Government services involving

(5) Electronic Government

(6) Elec other challenges to improve the
perform

(7) To tak better organization, improved interagency collaboration, and more focused
oversight

(b) PURPOSES-

(1) To provi ment services and processes by establishing an Administrator of a new Office of Electronic Government within the Office of Management
and Budget.

(2) To promot provide increased opportunities for citizen participation in Government.

(3) To promote electronic Government services, where this collaboration would improve the service to citizens by integrating related functions, and in the use of internal electronic Government processes,
where this colla the efficiency and effectiveness of the processes.

(4) To improve the ability of the Government to achieve agency missions and program performance goals.

(5) To promote the use of the Internet and emerging technologies within and across Government agencies to provide citizen-centric Government information and services.

(6) To reduce costs and burdens for businesses and other Government entities.

(7) To promote better informed decisionmaking by policy makers.

(8) To promote access to high quality Government information and services across multiple channels.

(9) To make the Federal Government more transparent and accountable.

(10) To transform agency operations by utilizing, where appropriate, best practices from public and private sector organizations.

(11) To provide enhanced access to Government information and services in a manner consistent with laws regarding protection of personal privacy, national security, records retention, access for persons with disabilities, and other relevant laws.

TITLE I--OFFICE OF MANAGEMENT AND BUDGET ELECTRONIC GOVERNMENT SERVICES

SEC. 101. MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES.

(a) IN GENERAL- Title 44, United States Code, is amended by inserting after chapter 35 the following:

`CHAPTER 36--MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

to improve the methods by which Government information, including information on the Internet, is organized, preserved, and made accessible to the public.

E-Government Act of 2002

→ **Start Points Often Dictate End Points** ←

Legislation introduced in 2001

For the purpose of bringing Government into the Information Age

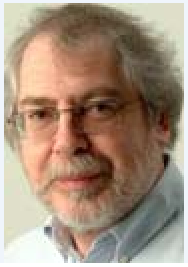
During a different Internet security era

That created an information security construct

That still governs today

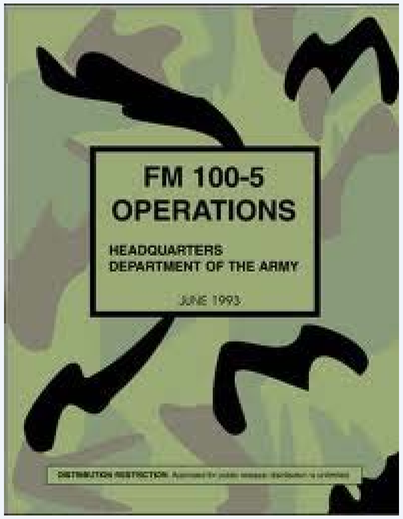
In a cybersecurity era

Security managers are chained to a backward-looking compliance treadmill that gives priority to old legacy practices, paperwork that no one reads, and outstanding audit actions from previous years.



"I'd love to now see it consigned to the scrap heap."

AirLand Battle Doctrine



FM 100-5
OPERATIONS

HEADQUARTERS
DEPARTMENT OF THE ARMY

JUNE 1993

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

Army’s View of Air Support

Close Air Support

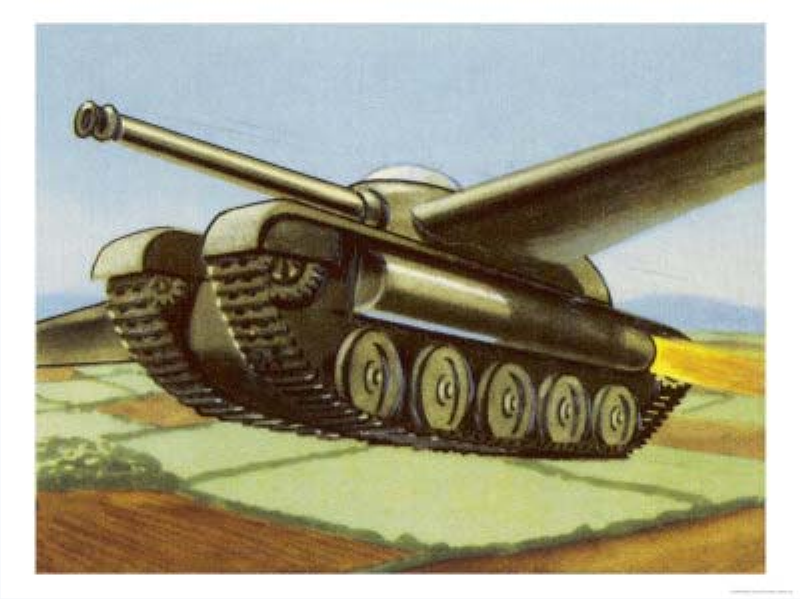
A-10 Thunderbolt

Air Force Culture

Close Air Support

F-16/A-16 Attack Variant

Army Culture



EXPLORING THE CONTOURS OF THE PRO

Contour Four:

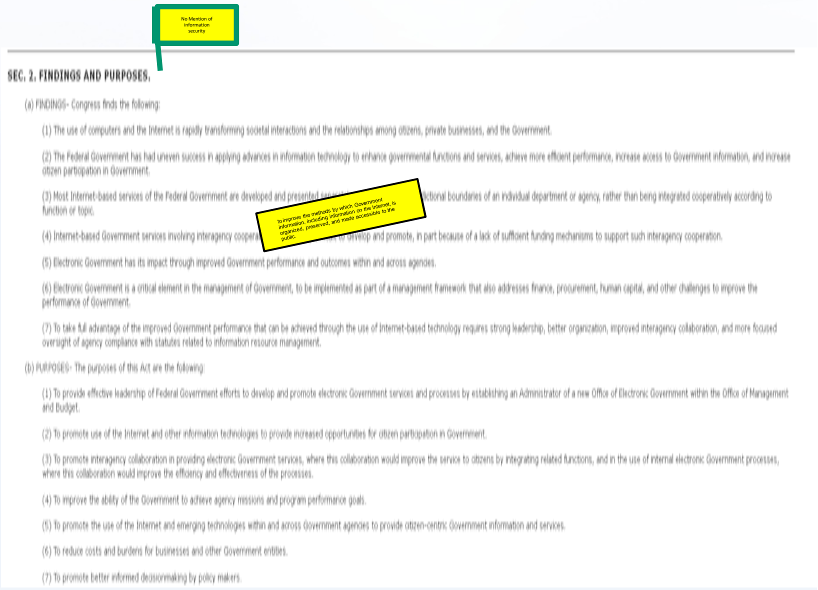
Applying the Wrong Model

Problematic Aspects

- **"Measurement Science" Approach to an Operational Problem**

- **Compliance/audit mindset**

- **Static Approach to a Dynamic Problem**



No Mention of information security

SEC. 2. FINDINGS AND PURPOSES.

(a) FINDINGS- Congress finds the following:

(1) The use of computers and the Internet is rapidly transforming societal interactions and the relationships among citizens, private businesses, and the Government.

(2) The Federal Government has had uneven success in applying advances in information technology to enhance governmental functions and services, achieve more efficient performance, increase access to Government information, and increase citizen participation in Government.

(3) Most Internet-based services of the Federal Government are developed and presented separat [illegible] ictional boundaries of an individual department or agency, rather than being integrated cooperatively according to function or topic.

to improve the methods by which Government information, including information on the Internet, is organized, preserved, and made accessible to the public.

(4) Internet-based Government services involving interagency coopera [illegible] to develop and promote, in part because of a lack of sufficient funding mechanisms to support such interagency cooperation.

(5) Electronic Government has its impact through improved Government performance and outcomes within and across agencies.

(6) Electronic Government is a critical element in the management of Government, to be implemented as part of a management framework that also addresses finance, procurement, human capital, and other challenges to improve the performance of Government.

(7) To take full advantage of the improved Government performance that can be achieved through the use of Internet-based technology requires strong leadership, better organization, improved interagency collaboration, and more focused oversight of agency compliance with statutes related to information resource management.

(b) PURPOSES- The purposes of this Act are the following:

(1) To provide effective leadership of Federal Government efforts to develop and promote electronic Government services and processes by establishing an Administrator of a new Office of Electronic Government within the Office of Management and Budget.

(2) To promote use of the Internet and other information technologies to provide increased opportunities for citizen participation in Government.

(3) To promote interagency collaboration in providing electronic Government services, where this collaboration would improve the service to citizens by integrating related functions, and in the use of internal electronic Government processes, where this collaboration would improve the efficiency and effectiveness of the processes.

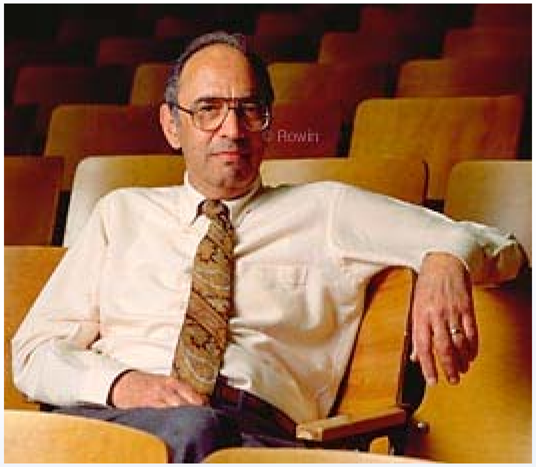
(4) To improve the ability of the Government to achieve agency missions and program performance goals.

(5) To promote the use of the Internet and emerging technologies within and across Government agencies to provide citizen-centric Government information and services.

(6) To reduce costs and burdens for businesses and other Government entities.

(7) To promote better informed decisionmaking by policy makers.

FINDING ANSWERS

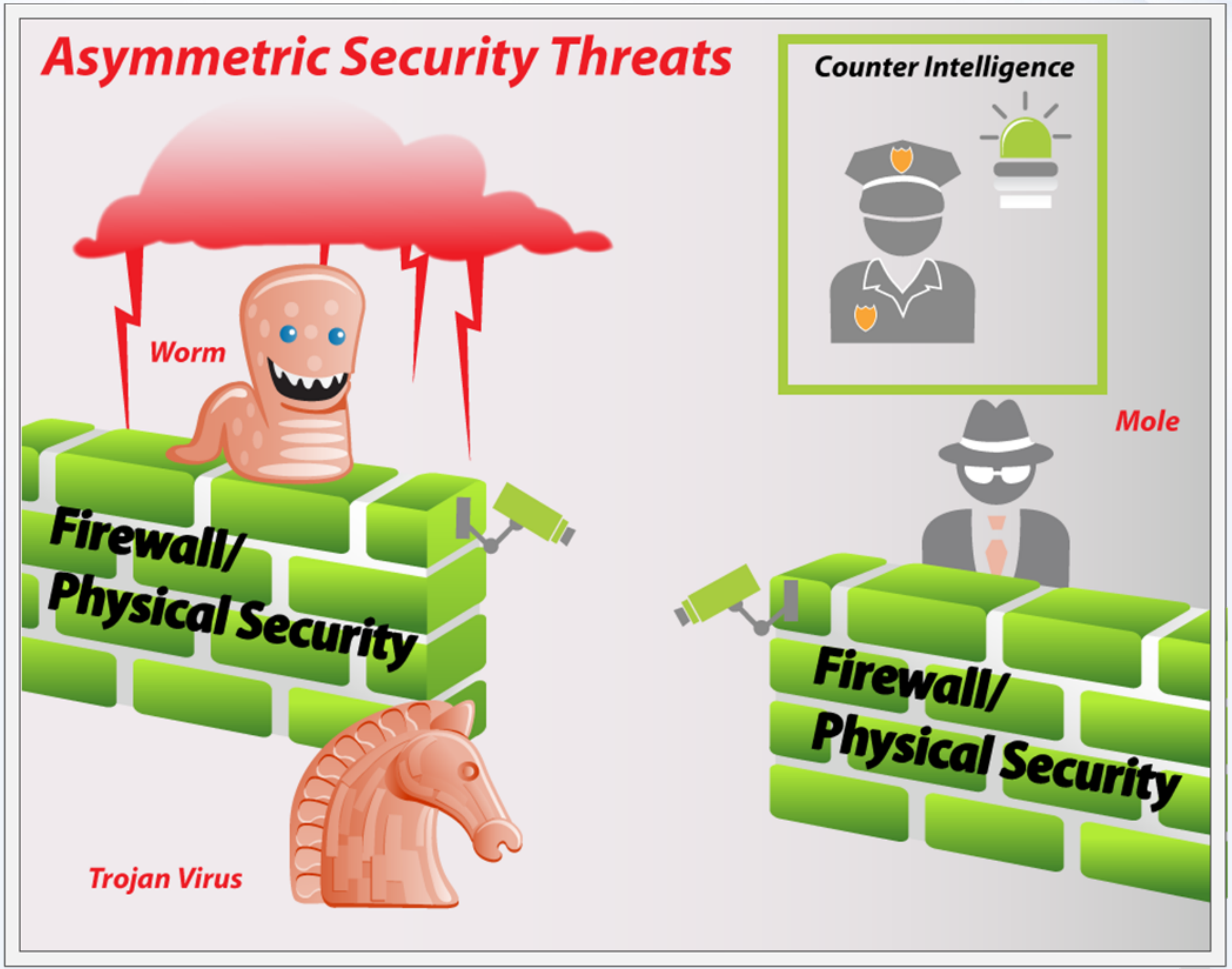


The Structure of Scientific Revolutions
Thomas Kuhn

‘one conceptual world view is replaced by another’

‘concensus emerges accepting a new framework’
- a new construct

- a NEW DISCIPLINE



Asymmetric Security Threats

FINDING ANSWERS

Toward a New Disciplinary Construct

- **Enables Cross-Disciplinary Integration**

- **New models emerge**

- **Appropriate application of science and policy, tailored to particular risks**

9/11 Commission Report

As presently configured, the national security institutions of the U.S. government are still the institutions constructed to win the Cold War. United States confronts a very different world today. Instead of facing a few very dangerous adversaries, the United States confronts a number of less visible challenges that surpass the boundaries of traditional nation-states and call for quick, imaginative, and agile responses.

*   *   *

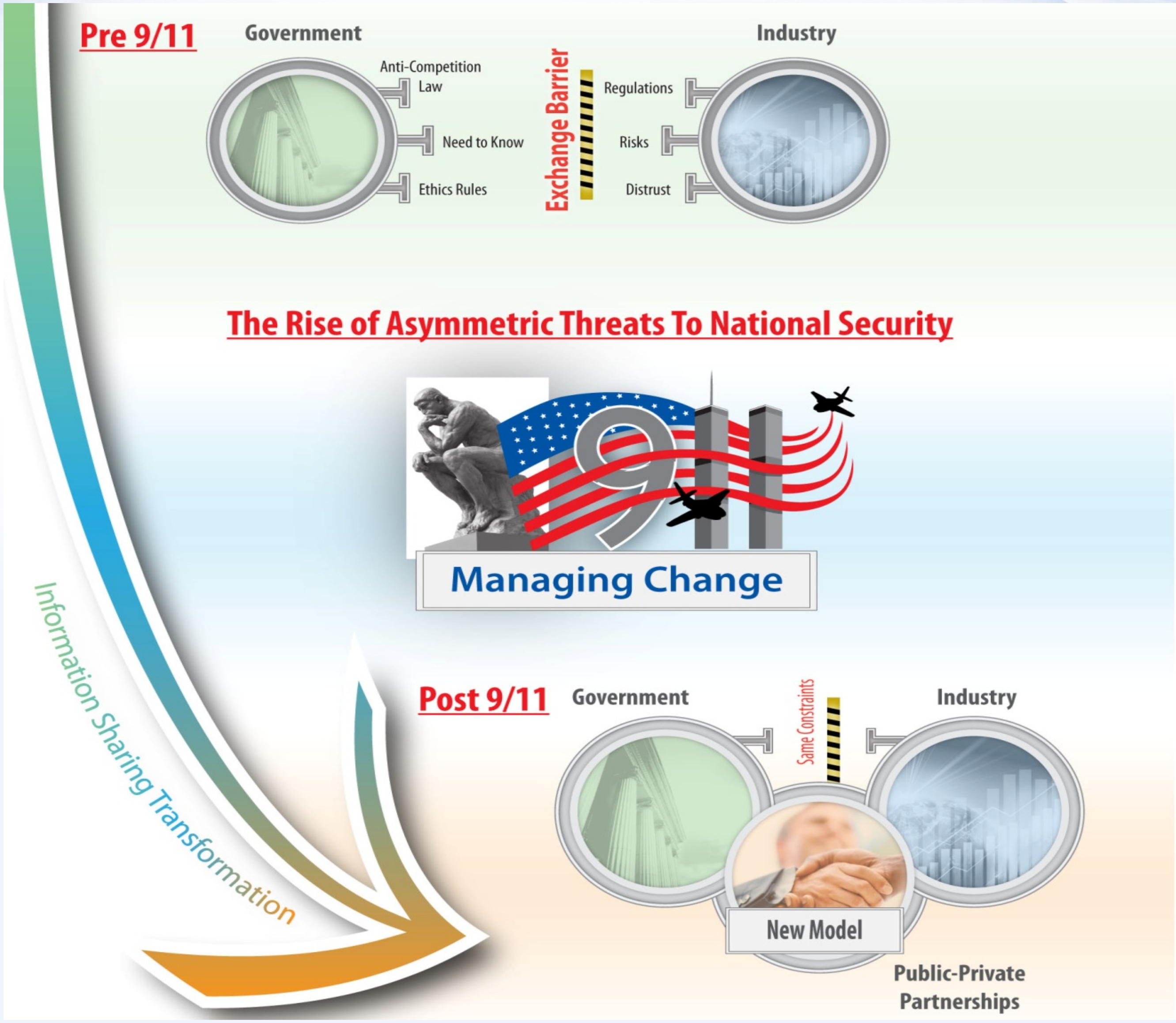
We recommend significant changes in the organization of the government. We know that the quality of the people is more important than the quality of the wiring diagrams.

*   *   *

The importance of integrated, allsource analysis cannot be overstated. Without it, it is not possible to "connect the dots." No one component holds all the relevant information.

*   *   *

We propose that information be shared horizontally, across new networks that transcend individual agencies.



Pre 9/11

Government

Anti-Competition Law

Need to Know

Ethics Rules

Exchange Barrier

Regulations

Risks

Distrust

Industry

The Rise of Asymmetric Threats To National Security

Managing Change

Information Sharing Transformation

Post 9/11

Government

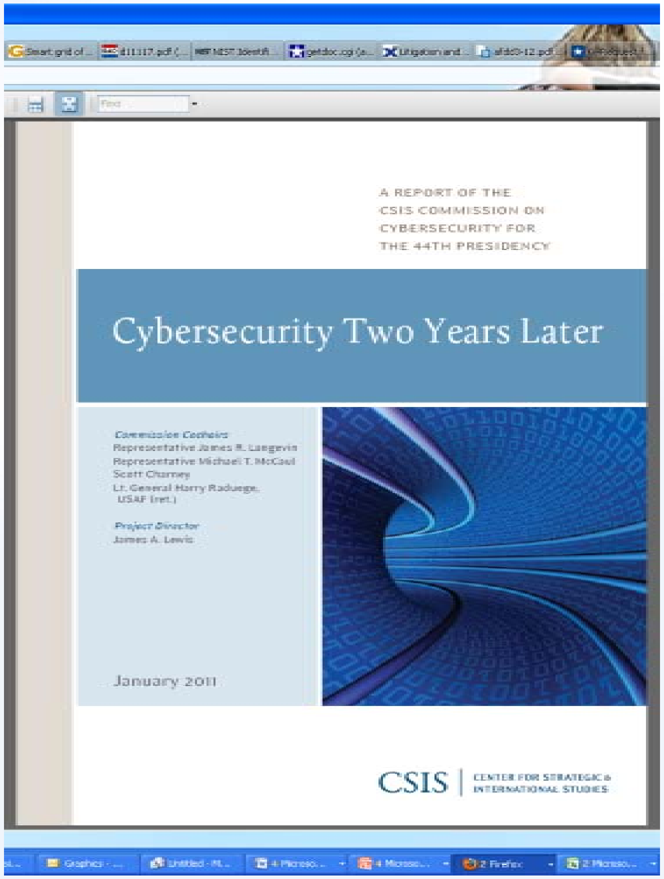
Same Constraints

Industry

New Model

Public-Private Partnerships

FINDING ANSWERS



A REPORT OF THE CSIS COMMISSION ON CYBERSECURITY FOR THE 44TH PRESIDENCY

Cybersecurity Two Years Later

Commission Cochairs
Representative James R. Langevin
Representative Michael T. McCaul
Scott Charney
Lt. General Harry Raduege, USAF (ret.)

Project Director
James A. Lewis

January 2011

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

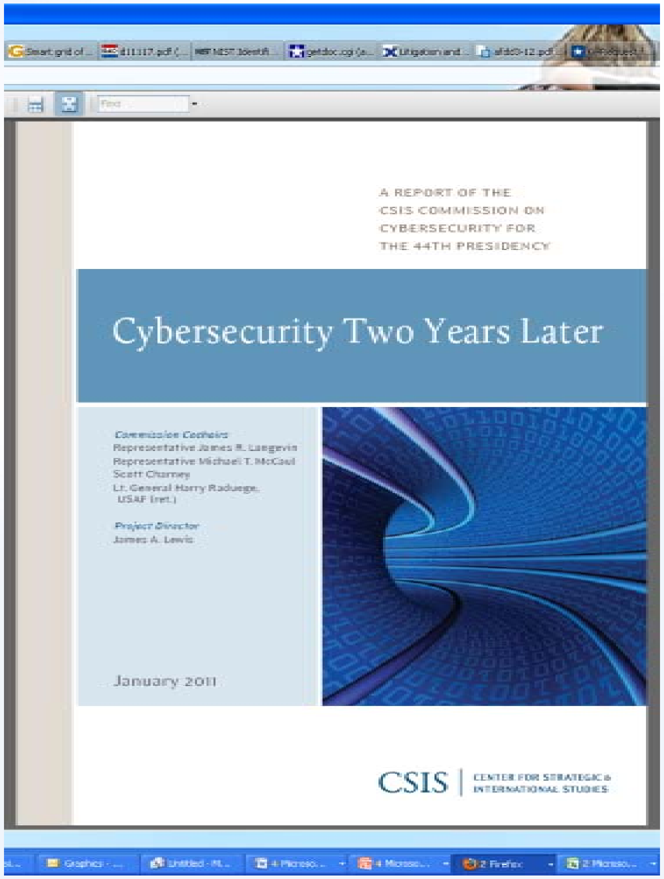
- Cybersecurity is now a major national security problem for the United States

- Decisions and actions must respect privacy and civil liberties

- Private initiative alone will not produce security

- Adopting a comprehensive national security strategy that embraces both the domestic and international aspects of cybersecurity will make us more secure

FINDING ANSWERS



A REPORT OF THE
CSIS COMMISSION ON
CYBERSECURITY FOR
THE 44TH PRESIDENCY

Cybersecurity Two Years Later

Commission Cochairs
Representative James R. Langevin
Representative Michael T. McCaul
Scott Charney
Lt. General Harry Raduege, USAF (ret.)

Project Director
James A. Lewis

January 2011

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

The cybersecurity debate is stuck. Many of the solutions still advocated for cybersecurity are well past their sell-by date. Public-private partnerships, information sharing, and self-regulation, are remedies we have tried for more than a decade without success. We need new concepts and new strategies if we are to reduce the risks in cyberspace to the United States.

Doug DePeppe
Managing Principal
i2IS Corporation
doug.depeppe@i2iscorp.com
www.i2iscorp.com
719-785-0355

THOUGHT LEADERSHIP STRATEGY RESEARCH TRAINING

9
Managing Change