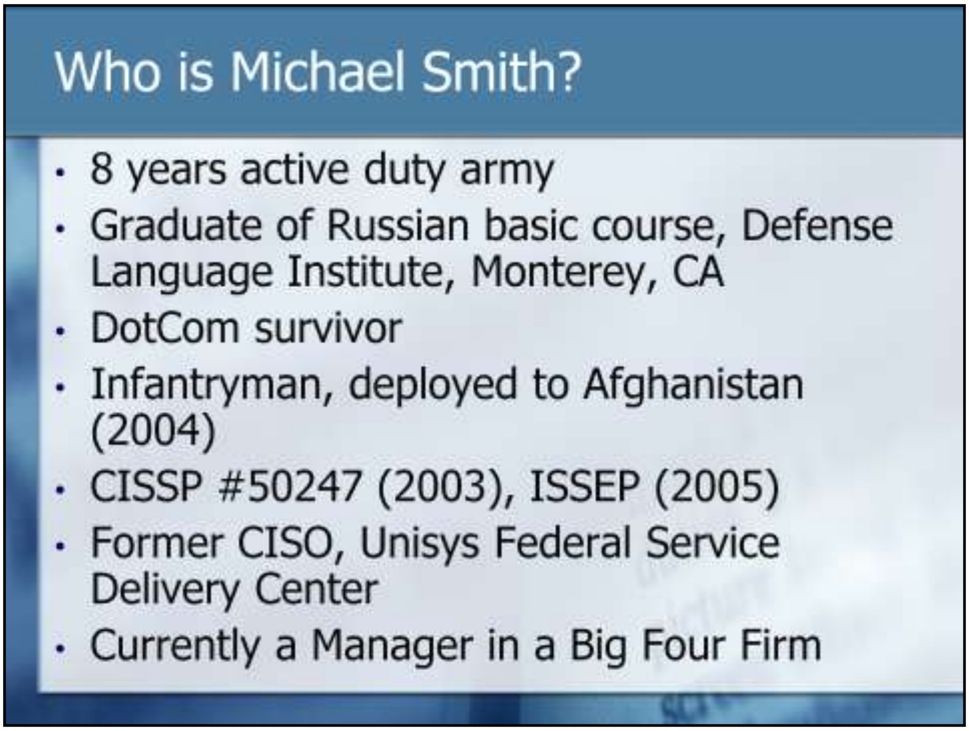
FISMA, NIST, and OMB Oh My!

Why information security in the US Federal Government fails or succeeds and what you can learn from it

The following presentation contains insights and opinions gathered from over 30 years of combined experience in the government INFOSEC space. It's interspersed with some humor – security presentations can be pretty dry without it.

We hope that this presentation will provide you with the impetus to reemphasize security within your organization, and feel good about doing so.



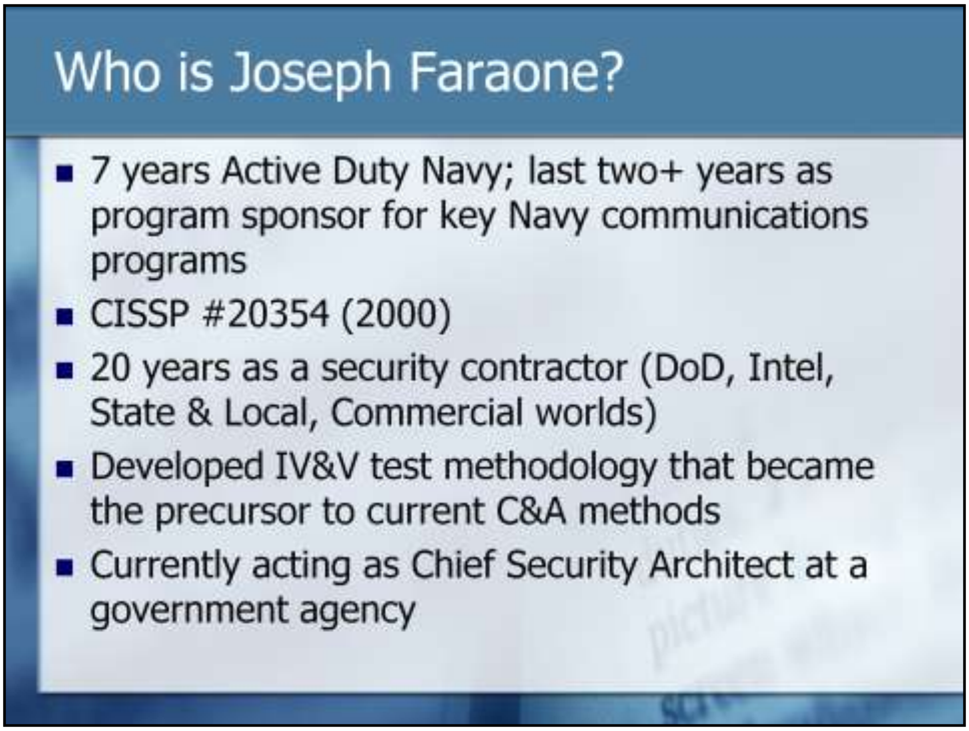
Who is Michael Smith?

- 8 years active duty army
- Graduate of Russian basic course, Defense Language Institute, Monterey, CA
- DotCom survivor
- Infantryman, deployed to Afghanistan (2004)
- CISSP #50247 (2003), ISSEP (2005)
- Former CISO, Unisys Federal Service Delivery Center
- Currently a Manager in a Big Four Firm

Mike’s blog is at http://www.guerilla-ciso.com/

Mike teaches for Potomac Forum http://www.potomacforum.org/

Contact information for Mike is at the end of this presentation.

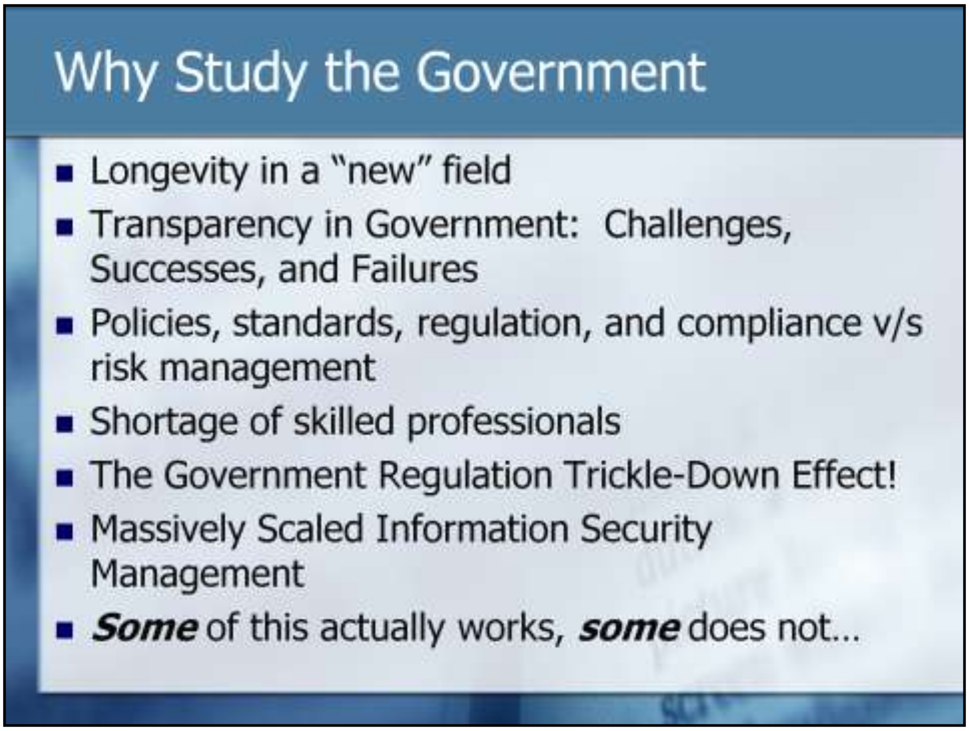


Who is Joseph Faraone?

- 7 years Active Duty Navy; last two+ years as program sponsor for key Navy communications programs
- CISSP #20354 (2000)
- 20 years as a security contractor (DoD, Intel, State & Local, Commercial worlds)
- Developed IV&V test methodology that became the precursor to current C&A methods
- Currently acting as Chief Security Architect at a government agency

Joe teaches for Potomac Forum http://www.potomacforum.org/ and often contributes to Mike’s blog.

Contact information for Joe is at the end of this presentation.

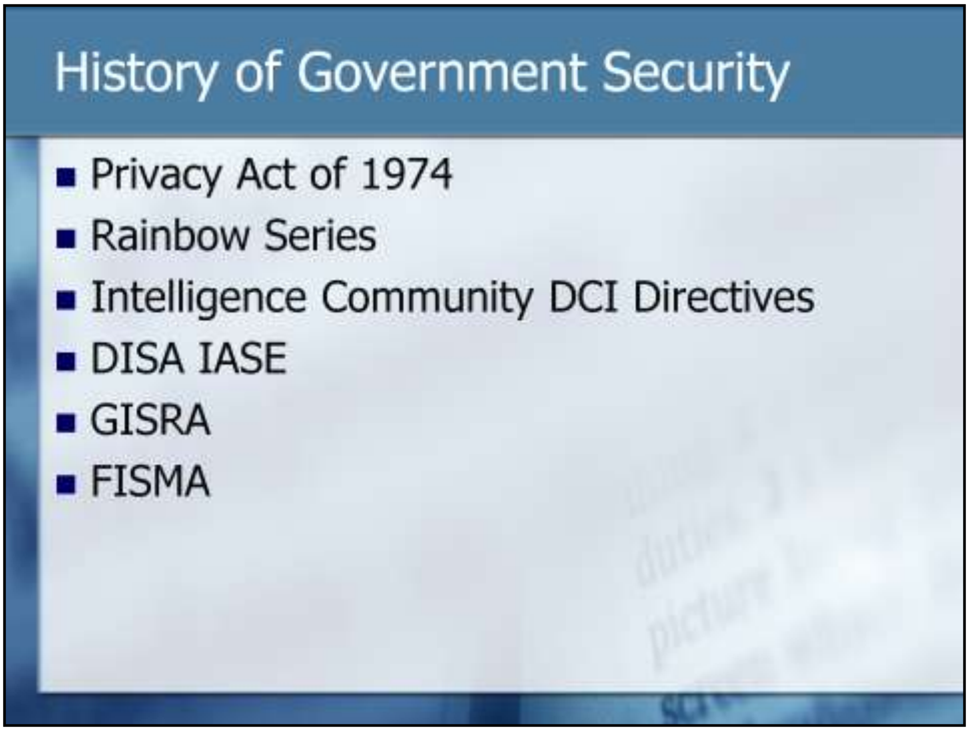


Why Study the Government

- Longevity in a “new” field
- Transparency in Government: Challenges, Successes, and Failures
- Policies, standards, regulation, and compliance v/s risk management
- Shortage of skilled professionals
- The Government Regulation Trickle-Down Effect!
- Massively Scaled Information Security Management
- ***Some*** of this actually works, ***some*** does not…

Typically Government security efforts are discounted as being for Government use only. The purpose of this presentation is to describe why it is important for security professionals to pay attention to what the Government is doing and learn from their successes and mistakes.

Understand, that Federal Government regulations have a nasty habit of working their way to the State and Local levels of government. Whatever your level of involvement with government and security, you would do well to get ahead of the curve.



History of Government Security

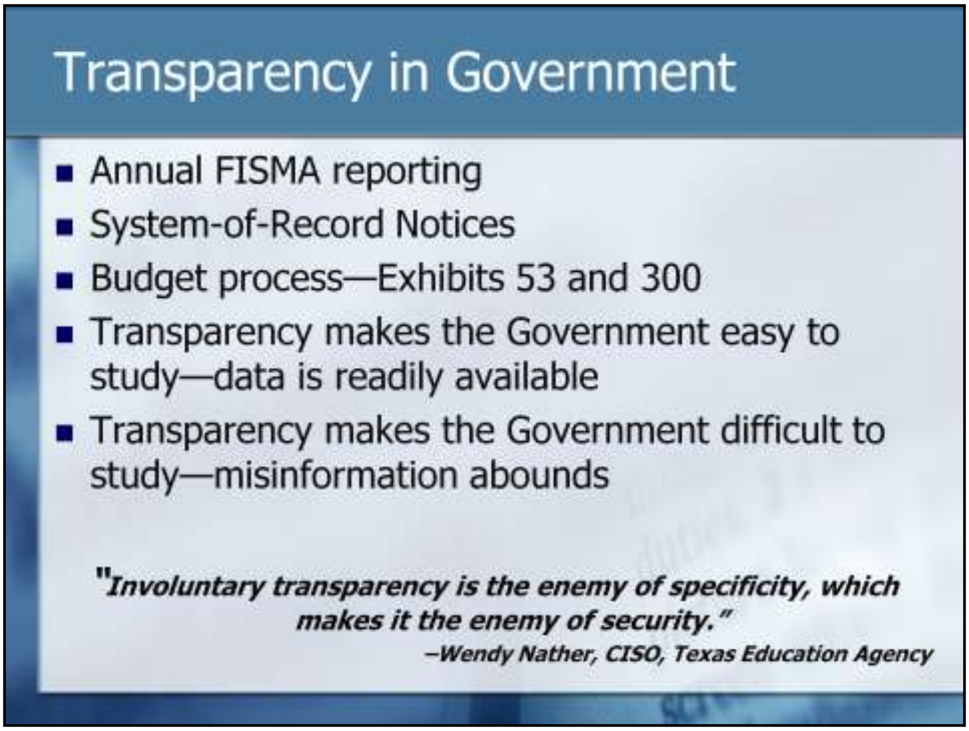
- Privacy Act of 1974
- Rainbow Series
- Intelligence Community DCI Directives
- DISA IASE
- GISRA
- FISMA

Government regulations around security have been with us for quite a while, and have gotten more specific and directive in nature over time. Their effectiveness is definitely open to debate, but the important thing is that government did recognize the importance of security and took steps to fill a perceived void.

Probably the most successful in their adoption have been FISMA and the Intel Community directives. These are the only ones with credible ”teeth.” Running afoul of the DCIDs will shut you down or send you to jail; FISMA can embarrass as well as strike an agency’s IT budget.

GISRA was a failure because it was strictly an accounting/paper exercise and didn’t force agencies to develop holistic security programs. Also, there were no standards for agencies to follow at the time.

Pointing at the DCIDs and the NSA Rainbow Series, these were effective in their time, but they were too system-centric in that they focused attention only on the computer systems and didn’t emphasize people, processes or procedures as much as their successors.



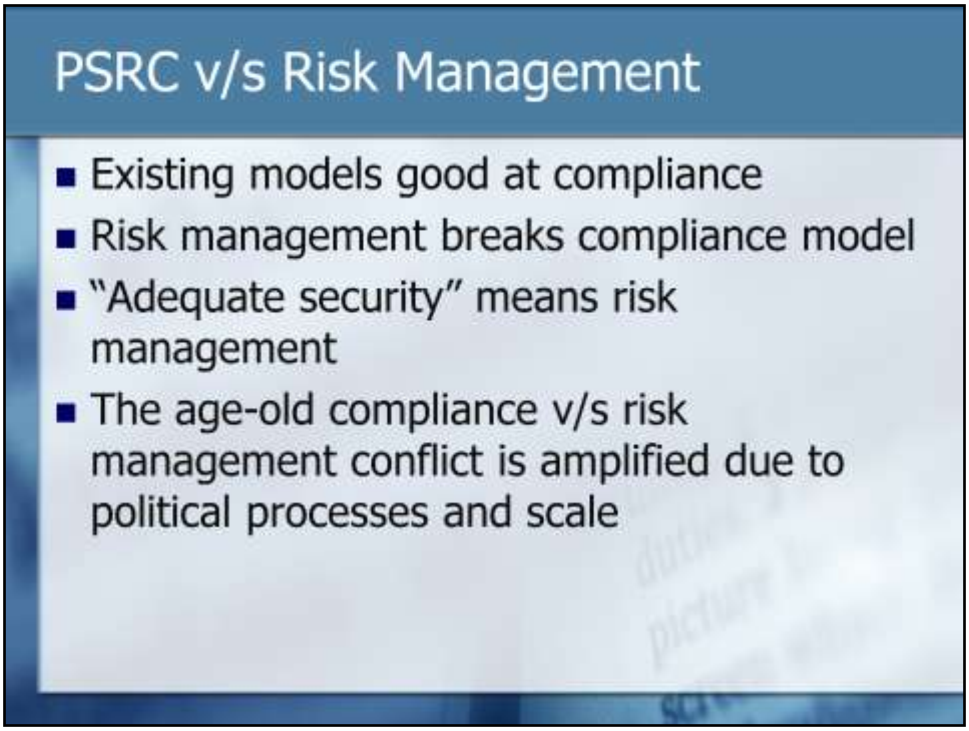
Transparency in Government

- Annual FISMA reporting
- System-of-Record Notices
- Budget process—Exhibits 53 and 300
- Transparency makes the Government easy to study—data is readily available
- Transparency makes the Government difficult to study—misinformation abounds

"Involuntary transparency is the enemy of specificity, which makes it the enemy of security."

–Wendy Nather, CISO, Texas Education Agency

Just like how data breach laws (SB 1386 and related) make it possible for researchers such as Adam Shostack (http://www.emergentchaos.com/) to study the impact of security incidents involving personally identifiable information (PII), the transparency of Government operations makes it easy to study from an information security management standpoint.



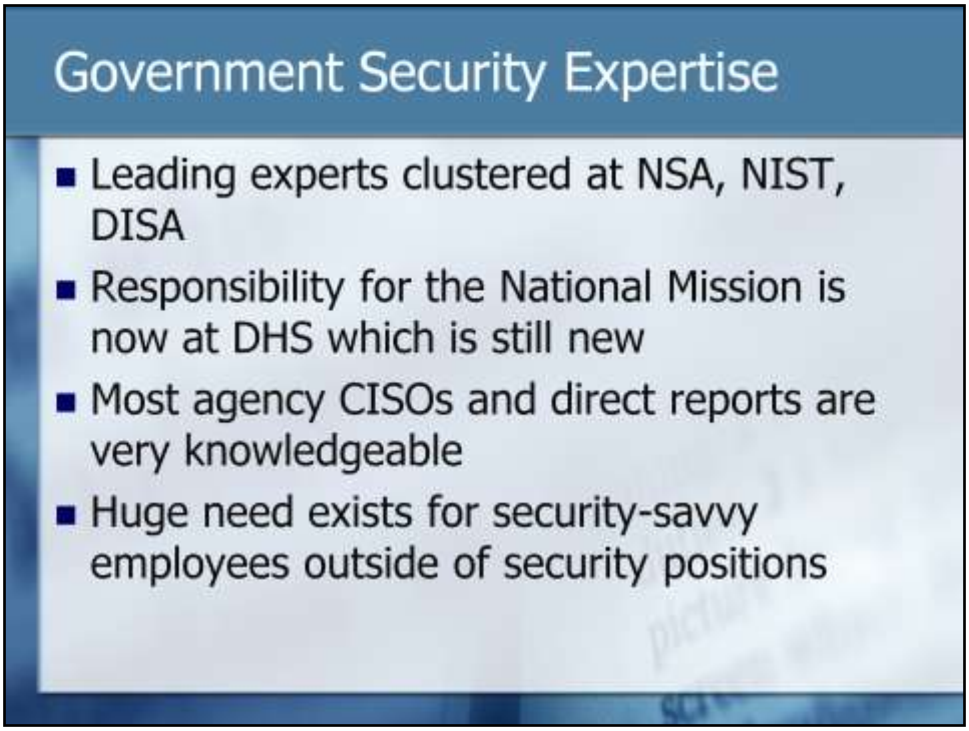
PSRC v/s Risk Management

- Existing models good at compliance
- Risk management breaks compliance model
- “Adequate security” means risk management
- The age-old compliance v/s risk management conflict is amplified due to political processes and scale

PSRC is “Policies, Standards, Regulations, and Compliance”.

We’ll talk more about models in a minute, but the important thing to remember is that all of our existing large-scale models are focused on compliance.

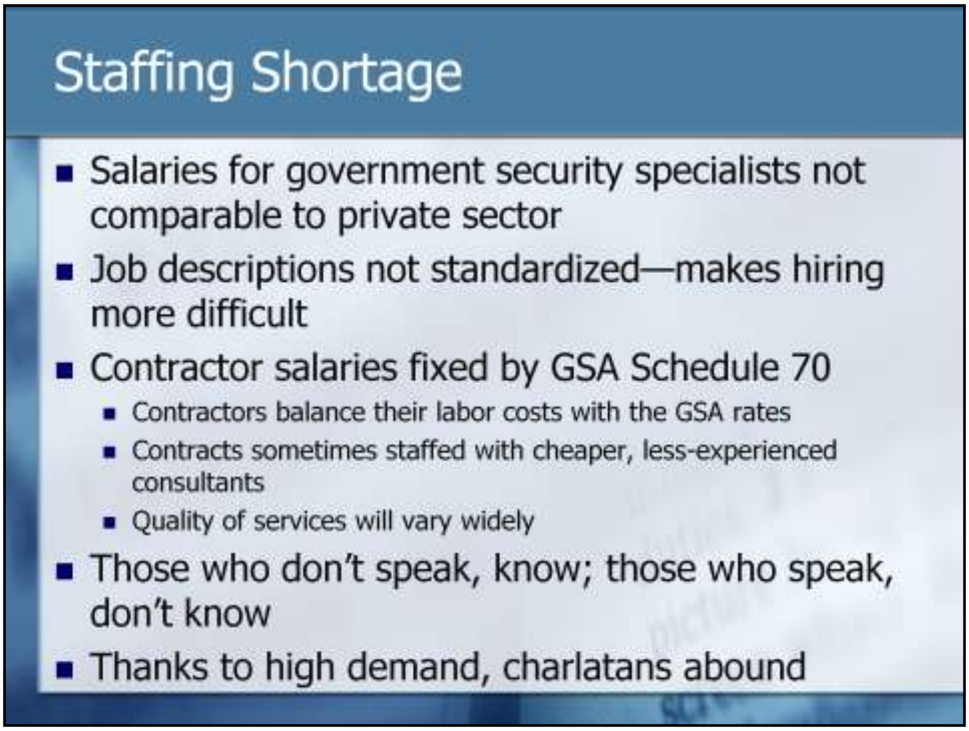
The term “Adequate Security” comes from OMB Circular A-130 and should be the aim of all security practitioners. Compliance models are aimed at risk avoidance as long as the risks are what the compliance framework anticipated.



Government Security Expertise

- Leading experts clustered at NSA, NIST, DISA
- Responsibility for the National Mission is now at DHS which is still new
- Most agency CISOs and direct reports are very knowledgeable
- Huge need exists for security-savvy employees outside of security positions

For the longest time, the Government has been the leader in information security. There still are isolated pockets of brilliance in the organizations we mention, and the aggregate level of security knowledge is increasing governmentwide.

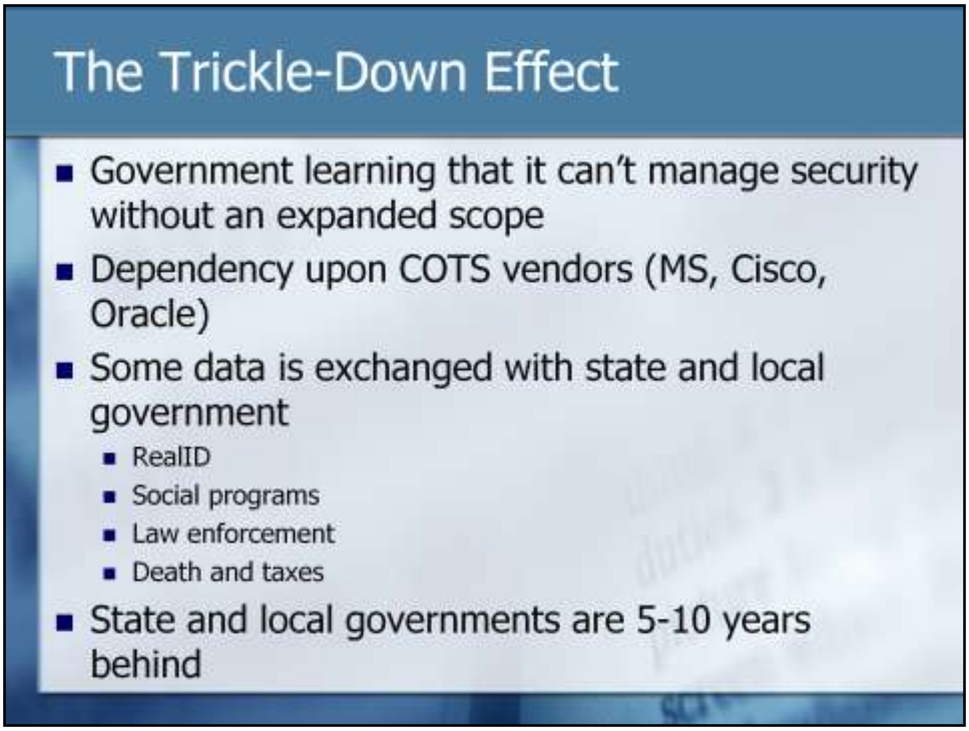


Staffing Shortage

- Salaries for government security specialists not comparable to private sector
- Job descriptions not standardized—makes hiring more difficult
- Contractor salaries fixed by GSA Schedule 70
  - Contractors balance their labor costs with the GSA rates
  - Contracts sometimes staffed with cheaper, less-experienced consultants
  - Quality of services will vary widely
- Those who don't speak, know; those who speak, don't know
- Thanks to high demand, charlatans abound

The staffing shortage is very critical, even more so because on top of the usual job requirements for a security practitioner, the Government security specialist also needs a certain level of “soft skills” and political awareness.

Geer testimony to Congress available at http://homeland.house.gov/SiteDocuments/20070425145243-10189.pdf

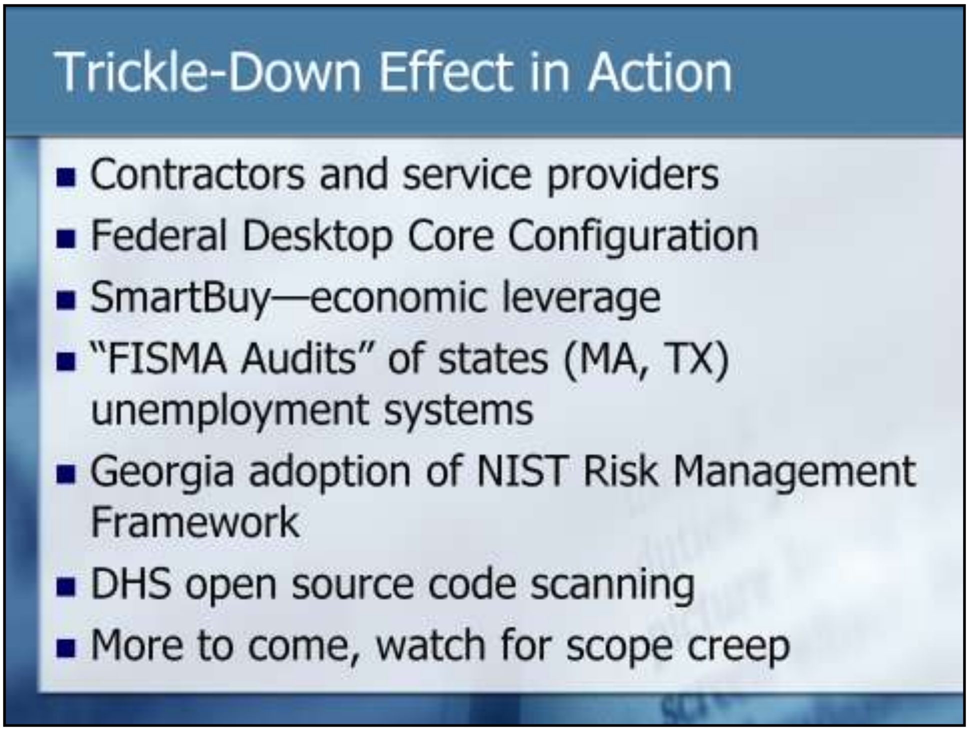


The Trickle-Down Effect

- Government learning that it can’t manage security without an expanded scope
- Dependency upon COTS vendors (MS, Cisco, Oracle)
- Some data is exchanged with state and local government
  - RealID
  - Social programs
  - Law enforcement
  - Death and taxes
- State and local governments are 5-10 years behind

The Trickle-Down effect is the part that you probably want to hear about—what benefits do you derive out of all this government experimentation?

Just like the war effort during World War II, eventually the scope of Government IT security needs to be expanded out to the private sector—the question is a matter of “how extensively, at what price, and who pays for it?”



Trickle-Down Effect in Action

- Contractors and service providers
- Federal Desktop Core Configuration
- SmartBuy—economic leverage
- "FISMA Audits" of states (MA, TX) unemployment systems
- Georgia adoption of NIST Risk Management Framework
- DHS open source code scanning
- More to come, watch for scope creep

While typical Government contracts now include the phrase "Contractor must be compliant with FISMA and all applicable NIST guidelines", there is much to be improved here. However, contractors are becoming more involved in securing Government IT systems.

FDCC is a hardening guide for desktops that is mandated by OMB and based on the DISA Windows XP and Vista STIGS. Eventually hardened versions will be available from OEM vendors and software applications will not be purchased by the Government unless they are certified to work on the FDCC image.

SmartBuy is a GSA program to bulk-purchase software.

http://www.gsa.gov/smartbuy

MA and TX FISMA Audit information from DOL:

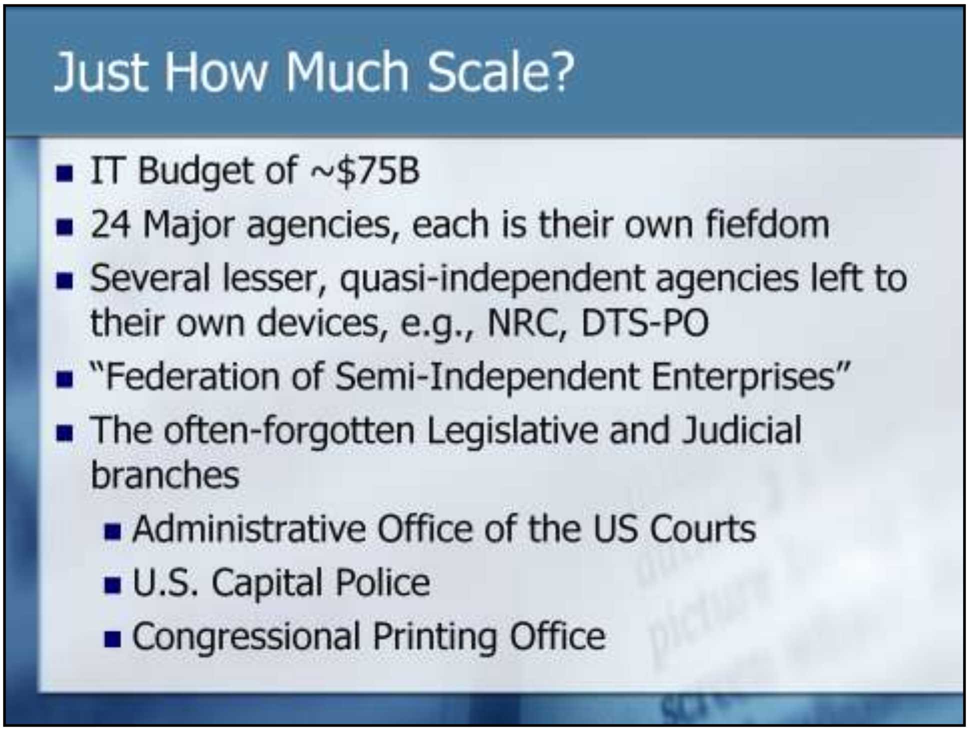
http://www.oig.dol.gov/public/semiannuals/54.pdf

Georgia has adopted FISMA-like reporting and the NIST SP documents.

http://www.govtech.com/gt/articles/277150

http://www.gta.georgia.gov/00/channel_title/0,2094,1070969_107916049,00.html

DHS sponsors an open-source code scanning project called SCAN. More information at: http://scan.coverity.com/about.html

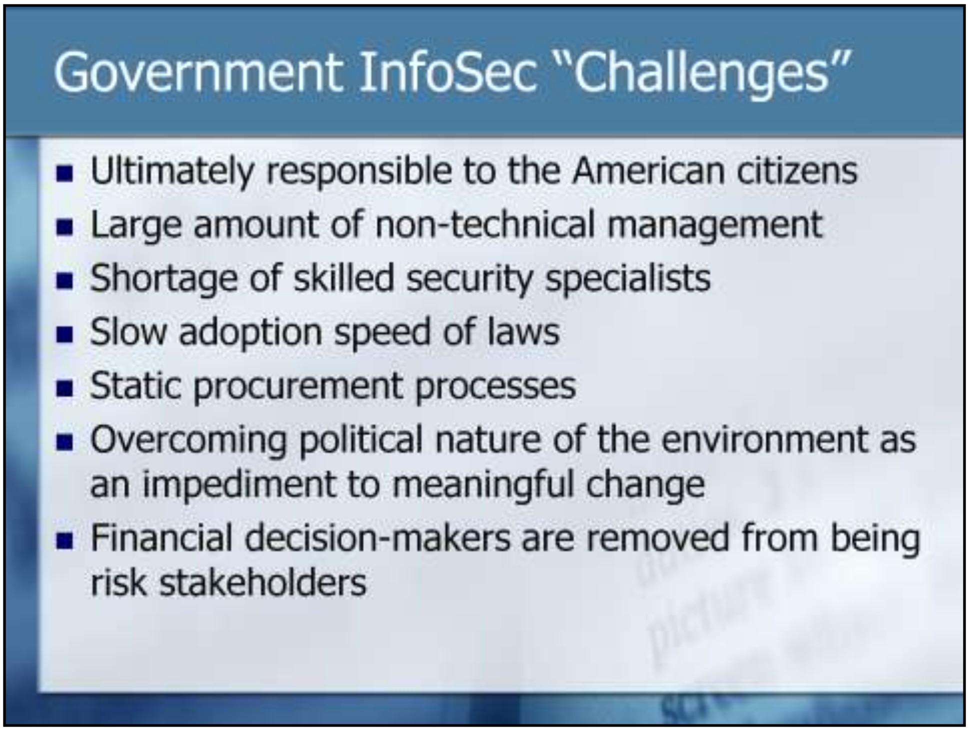


Just How Much Scale?

- IT Budget of ~$75B
- 24 Major agencies, each is their own fiefdom
- Several lesser, quasi-independent agencies left to their own devices, e.g., NRC, DTS-PO
- “Federation of Semi-Independent Enterprises”
- The often-forgotten Legislative and Judicial branches
  - Administrative Office of the US Courts
  - U.S. Capital Police
  - Congressional Printing Office

The primary problem facing the Government is one of massive scale when almost all security methodology is at the enterprise and below. We’ll talk about scaling up existing governance models later on in this presentation.

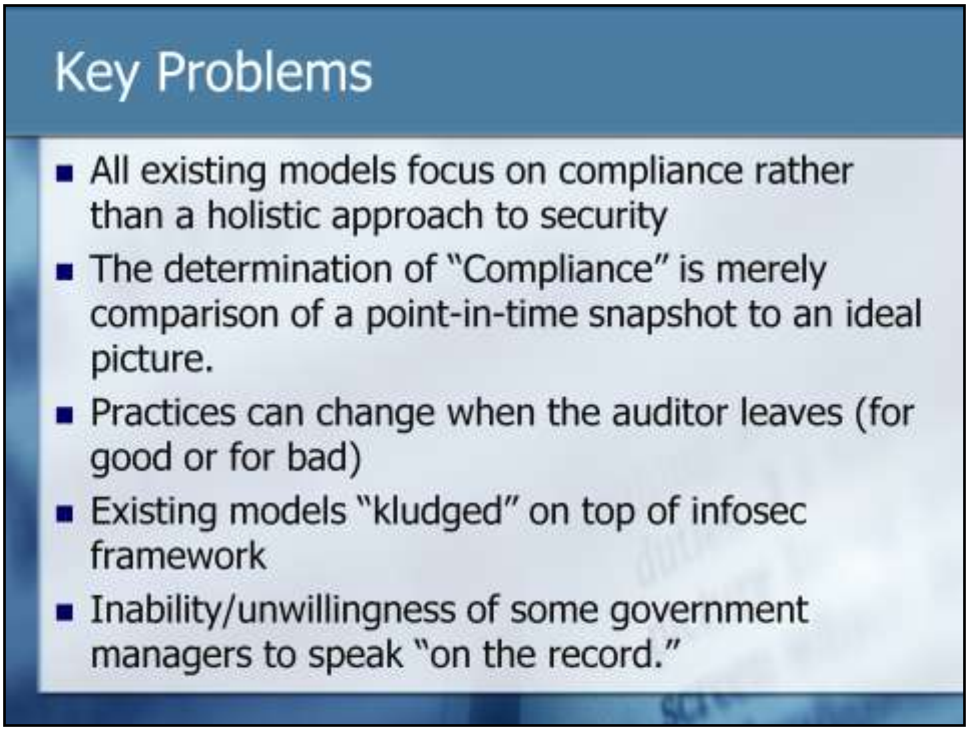
The only realistic approach is to make agency heads accountable for implementation of security within their organizations following guidance that must be applicable across government. A pretty daunting prospect, but the guidance is one that NIST has done well considering the environment that they work in.



Government InfoSec "Challenges"

- Ultimately responsible to the American citizens
- Large amount of non-technical management
- Shortage of skilled security specialists
- Slow adoption speed of laws
- Static procurement processes
- Overcoming political nature of the environment as an impediment to meaningful change
- Financial decision-makers are removed from being risk stakeholders

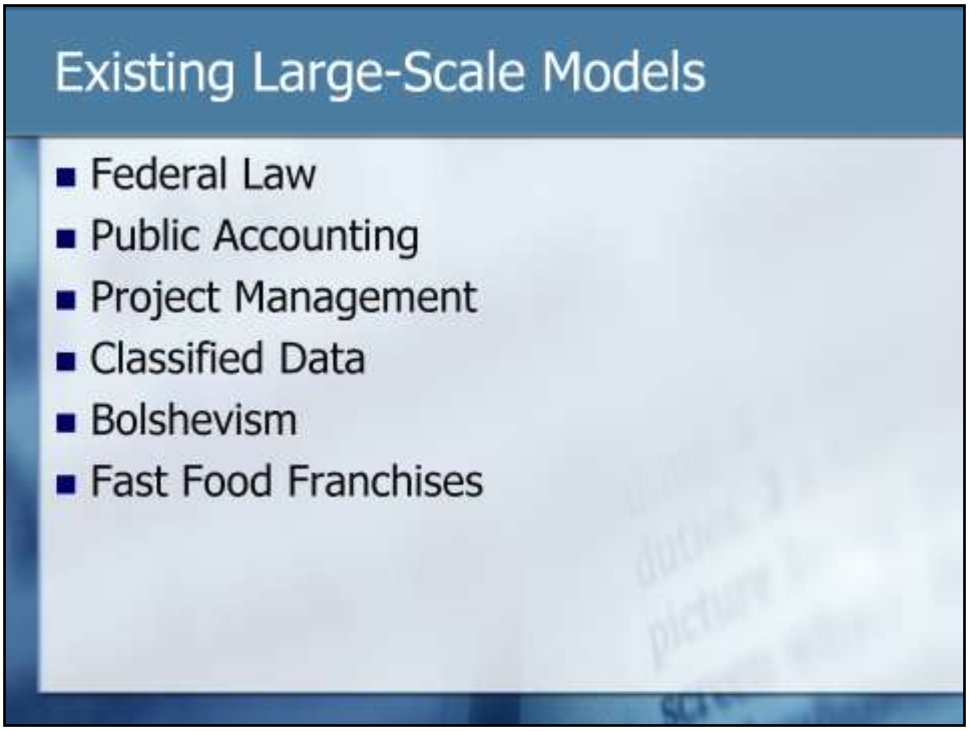
As we'll see when we start talking about security models, the primary problem of the Government is one of scale, and all of the challenges faced by the Government stem from it.



Key Problems

- All existing models focus on compliance rather than a holistic approach to security
- The determination of "Compliance" is merely comparison of a point-in-time snapshot to an ideal picture.
- Practices can change when the auditor leaves (for good or for bad)
- Existing models "kludged" on top of infosec framework
- Inability/unwillingness of some government managers to speak "on the record."

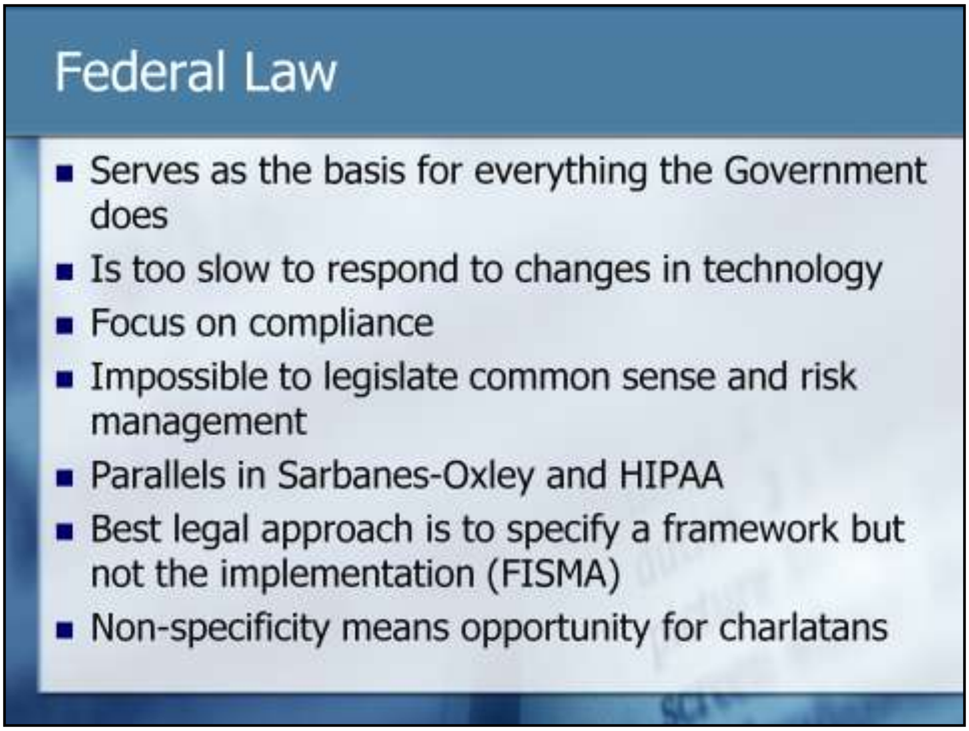
One thing that we have discovered/realized is that best practices are best practices. Regulatory frameworks like Sarbanes-Oxley, NIST Publications CoBIT, FISCAM, DITSCAP, and ISO17799 all strive to accomplish the same thing – defining controls to implement holistic security and governance for the enterprise whether government or private sector. One need look no further than Appendix G of the 800-53 for "proof" of this concept.



Existing Large-Scale Models

- Federal Law
- Public Accounting
- Project Management
- Classified Data
- Bolshevism
- Fast Food Franchises

We'll go through each of these in a minute.



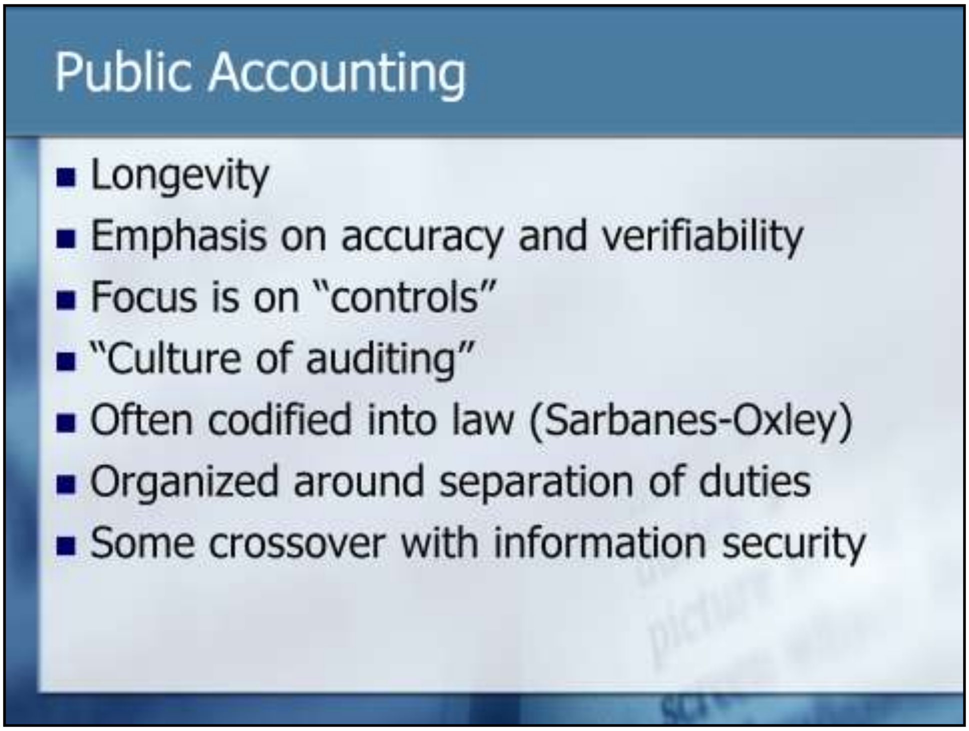
Federal Law

- Serves as the basis for everything the Government does
- Is too slow to respond to changes in technology
- Focus on compliance
- Impossible to legislate common sense and risk management
- Parallels in Sarbanes-Oxley and HIPAA
- Best legal approach is to specify a framework but not the implementation (FISMA)
- Non-specificity means opportunity for charlatans

“To retain respect for sausages and laws, one must not watch them in the making.” –Otto von Bismarck

Law is the only thing that has substantial penalties. The problem is that laws cannot effectively keep up with the rapid pace of security technology. Because of this, the only approach that works is small-scope laws that specify a framework such as what FISMA has done with requiring security planning, risk assessment, contingency planning, and security testing. Of course, this leaves a considerable amount of flexibility which means opportunity for poor execution.

BOLD STATEMENT: (“hear me now, believe me later…”) The greater/deeper your understanding of the fundamentals of security best/leading practices, the framework becomes less important.   At the point of highest achievement, understanding or “enlightenment,” the frameworks devolve to a matter of reporting.

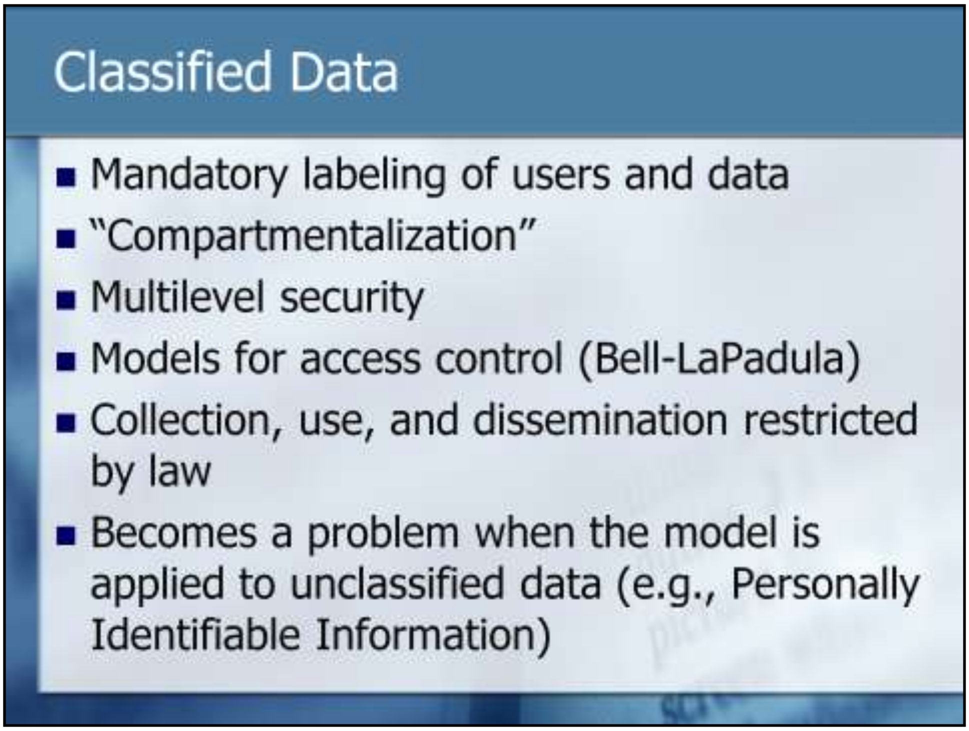


Public Accounting

- Longevity
- Emphasis on accuracy and verifiability
- Focus is on “controls”
- “Culture of auditing”
- Often codified into law (Sarbanes-Oxley)
- Organized around separation of duties
- Some crossover with information security

Public accounting has some crossovers into information security and is “typically” aimed at fraud prevention although at some levels it has an element of quantitative risk management.

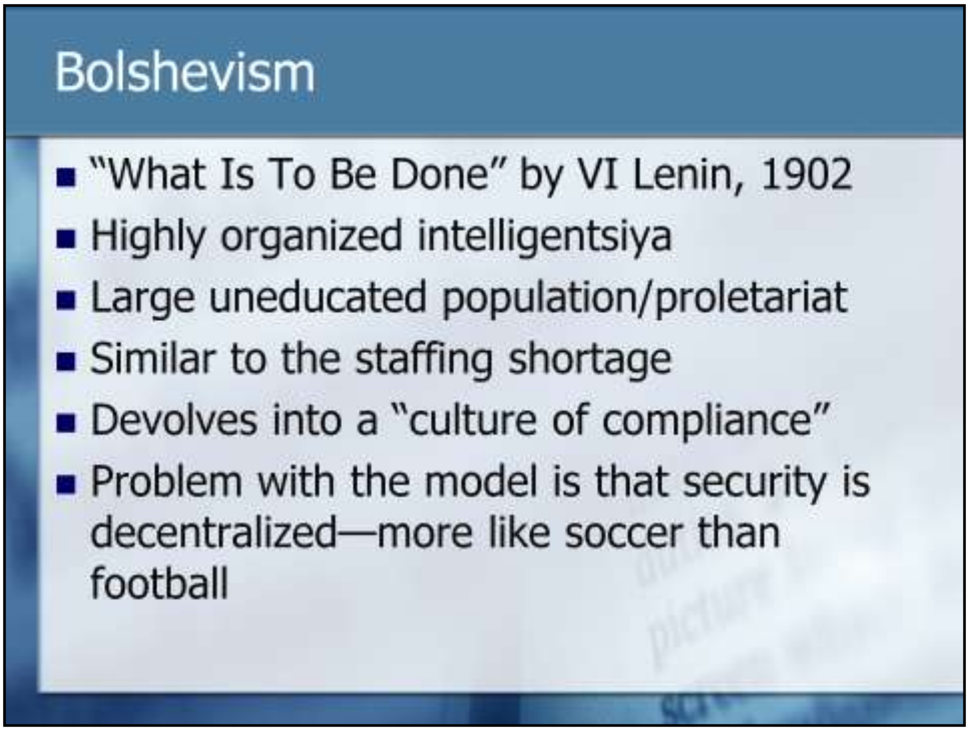
In some ways, security in the Government is controlled by accountants (as it should be, since security is economics): OMB and GAO.



Classified Data

- Mandatory labeling of users and data
- "Compartmentalization"
- Multilevel security
- Models for access control (Bell-LaPadula)
- Collection, use, and dissemination restricted by law
- Becomes a problem when the model is applied to unclassified data (e.g., Personally Identifiable Information)

Classified data and the laws and regulations behind it is something interesting to study due to the level of penalties for disclosure of information. Most of the ur-thought around security management such as the rainbow series was designed to protect classified data.

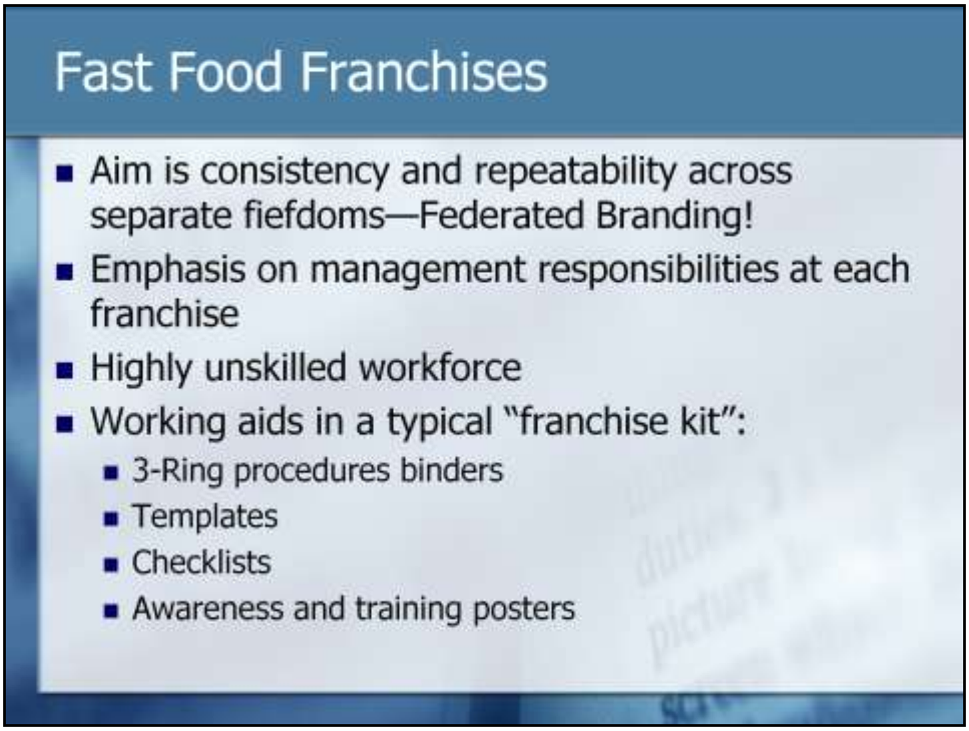


Bolshevism

- "What Is To Be Done" by VI Lenin, 1902
- Highly organized intelligentsiya
- Large uneducated population/proletariat
- Similar to the staffing shortage
- Devolves into a "culture of compliance"
- Problem with the model is that security is decentralized—more like soccer than football

Bolshevism is a model where a cadre of highly-organized intelligentsiya take over the country for the sake of the populace who do not know what they want.

What does this have to do with security in the Government? Well, when you have a personality shortage, this is what becomes the de-facto governance model.

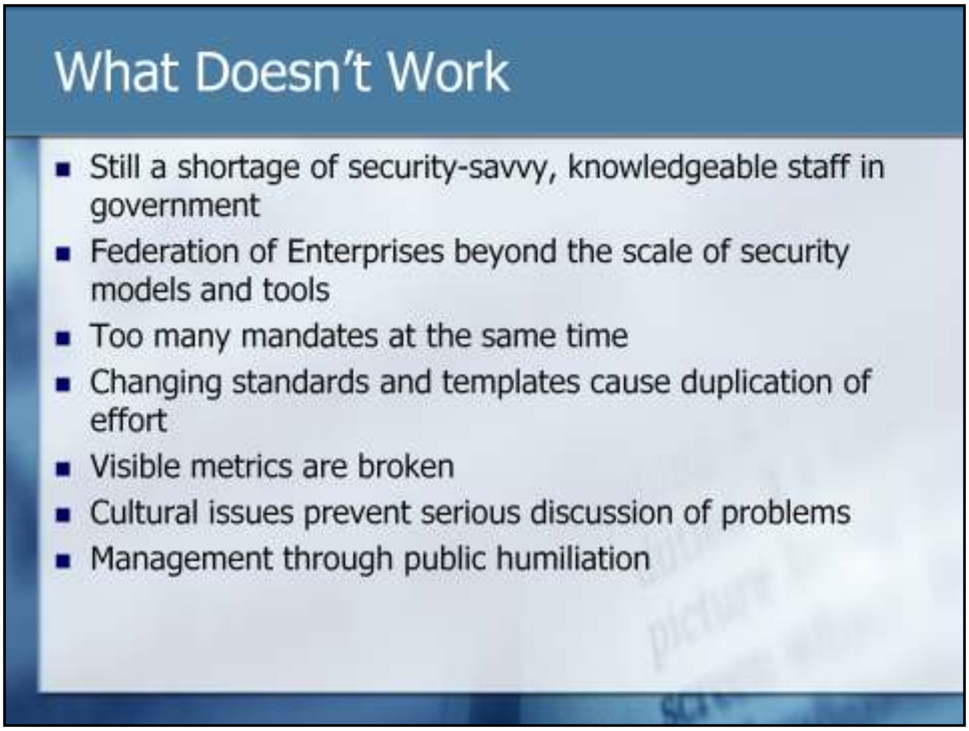


Fast Food Franchises

- Aim is consistency and repeatability across separate fiefdoms—Federated Branding!
- Emphasis on management responsibilities at each franchise
- Highly unskilled workforce
- Working aids in a typical "franchise kit":
  - 3-Ring procedures binders
  - Templates
  - Checklists
  - Awareness and training posters

Fast food franchises are vastly standardized.

Ideally in Government we would like to be able to write one set of policy, standards, and regulations and make them applicable across the entire government—all three branches—in order to reduce the amount of translation that needs to happen from one agency to the next. In practice, however, this has proven difficult to do because of the wide variety of missions and organizational structures that agencies support.



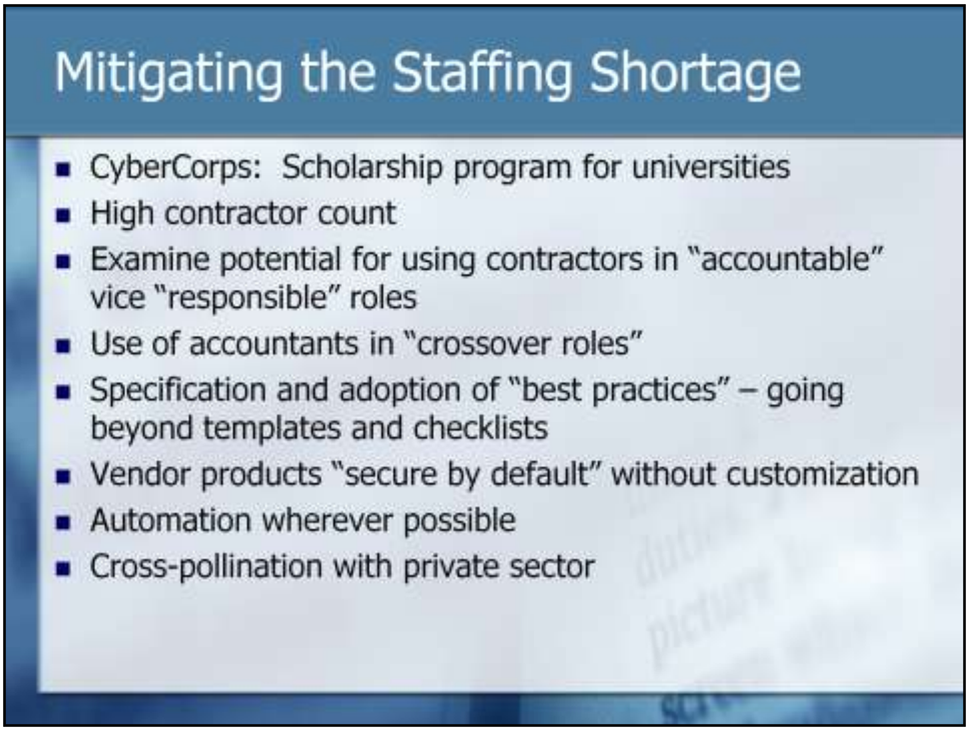
What Doesn’t Work

- Still a shortage of security-savvy, knowledgeable staff in government
- Federation of Enterprises beyond the scale of security models and tools
- Too many mandates at the same time
- Changing standards and templates cause duplication of effort
- Visible metrics are broken
- Cultural issues prevent serious discussion of problems
- Management through public humiliation

Department of Labor indicates that for the foreseeable future, the curve of demand is growing faster than the curve of supply of security professionals. So, the shortage gap is increasing at an increasing rate, implying significant salary pressure and more demanding and stressful work environments.

Likewise, there are additional pressures on the “knowledgeable staff”. For example, there is pressure for professional certification, certification maintenance, and knowledge of ever increasing technologies and requirements.

There is also pressure toward job/responsibility and job enlargement. For example, Privacy specialists.

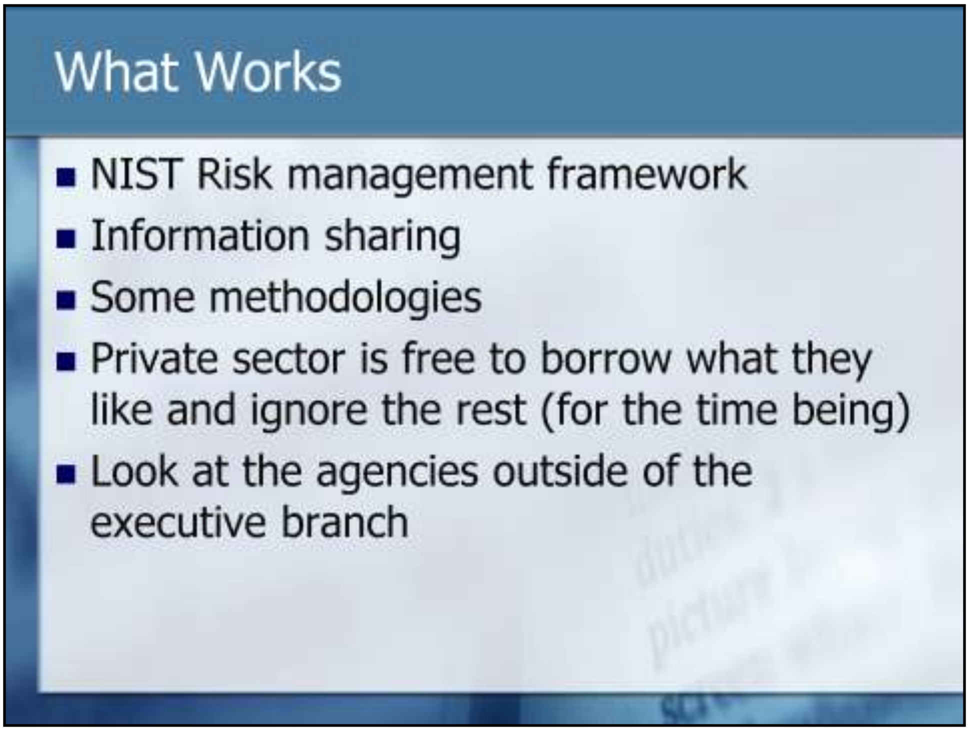


Mitigating the Staffing Shortage

- CyberCorps: Scholarship program for universities
- High contractor count
- Examine potential for using contractors in "accountable" vice "responsible" roles
- Use of accountants in "crossover roles"
- Specification and adoption of "best practices" – going beyond templates and checklists
- Vendor products "secure by default" without customization
- Automation wherever possible
- Cross-pollination with private sector

As much as you think this presentation is about how you can use some tactics, techniques, and procedures, this presentation is really about how you can help the Government. Due to the limitations that the Government has in flexibility, staffing, and technological expertise, the only way for us to succeed is to draw upon resources in the private sector. Part of this is the cause for the “trickle-down effect” that we’ve discussed.

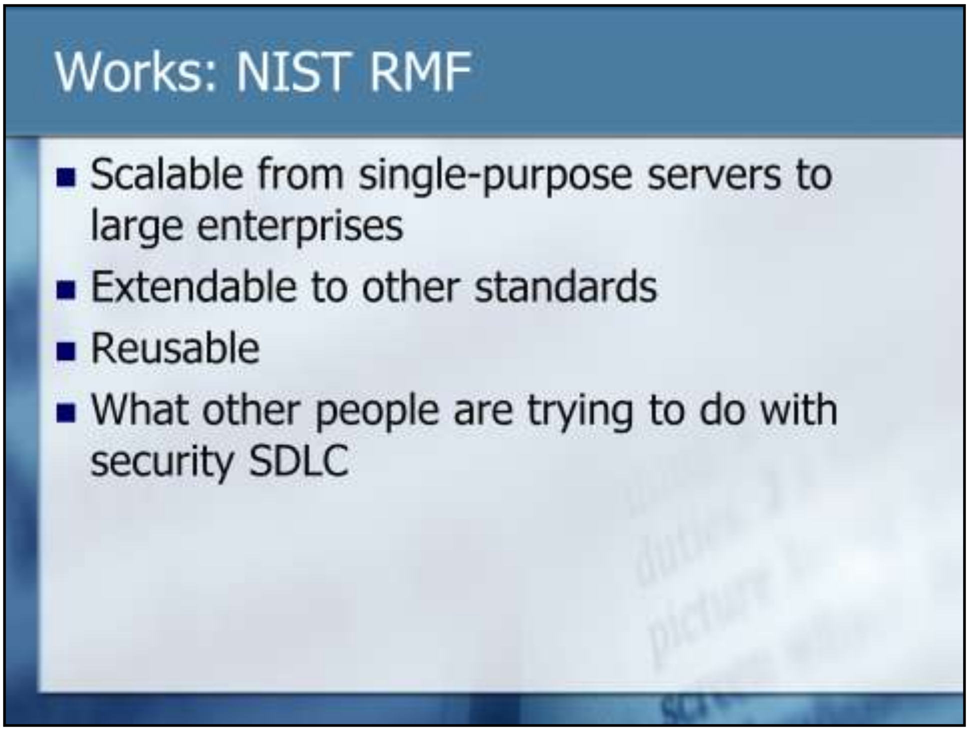
Note that some of these techniques are not applicable only to Government.



What Works

- NIST Risk management framework
- Information sharing
- Some methodologies
- Private sector is free to borrow what they like and ignore the rest (for the time being)
- Look at the agencies outside of the executive branch

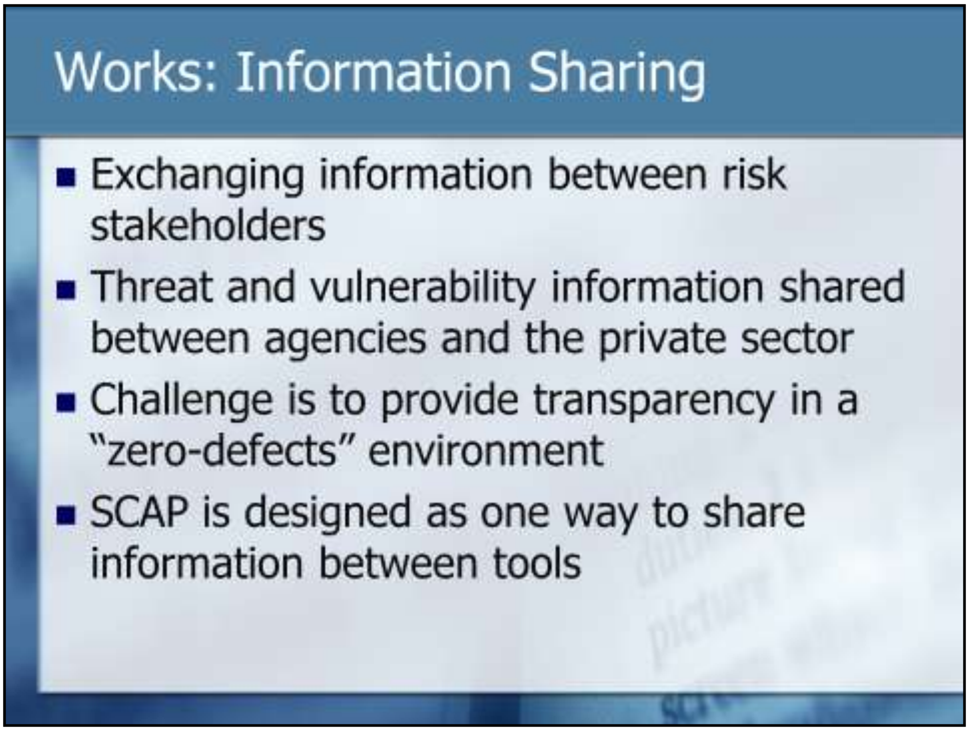
We’ll go through each one of these items.



Works: NIST RMF

- Scalable from single-purpose servers to large enterprises
- Extendable to other standards
- Reusable
- What other people are trying to do with security SDLC

http://csrc.nist.gov/groups/SMA/fisma/framework.html

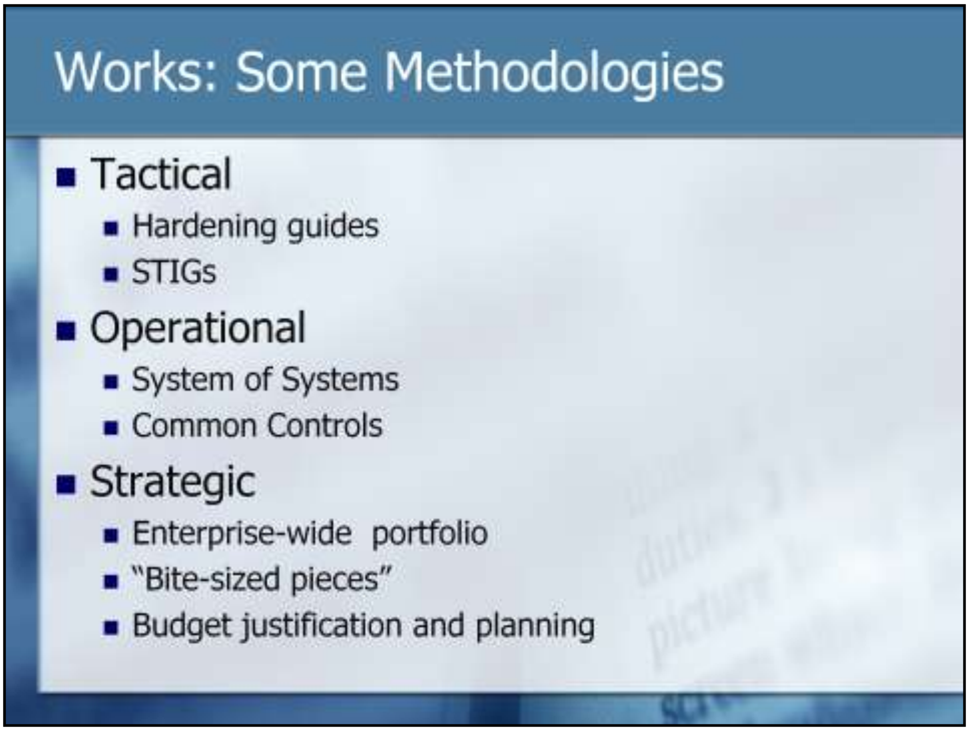


Works: Information Sharing

- Exchanging information between risk stakeholders
- Threat and vulnerability information shared between agencies and the private sector
- Challenge is to provide transparency in a “zero-defects” environment
- SCAP is designed as one way to share information between tools

The endstate of the NIST Risk Management Framework is transparency between risk stakeholders. While some of this happens, much more is needed.

SCAP is the Security Content Automation Protocol. More information is at http://nvd.nist.gov/scap.cfm



Works: Some Methodologies

- Tactical
  - Hardening guides
  - STIGs
- Operational
  - System of Systems
  - Common Controls
- Strategic
  - Enterprise-wide portfolio
  - "Bite-sized pieces"
  - Budget justification and planning

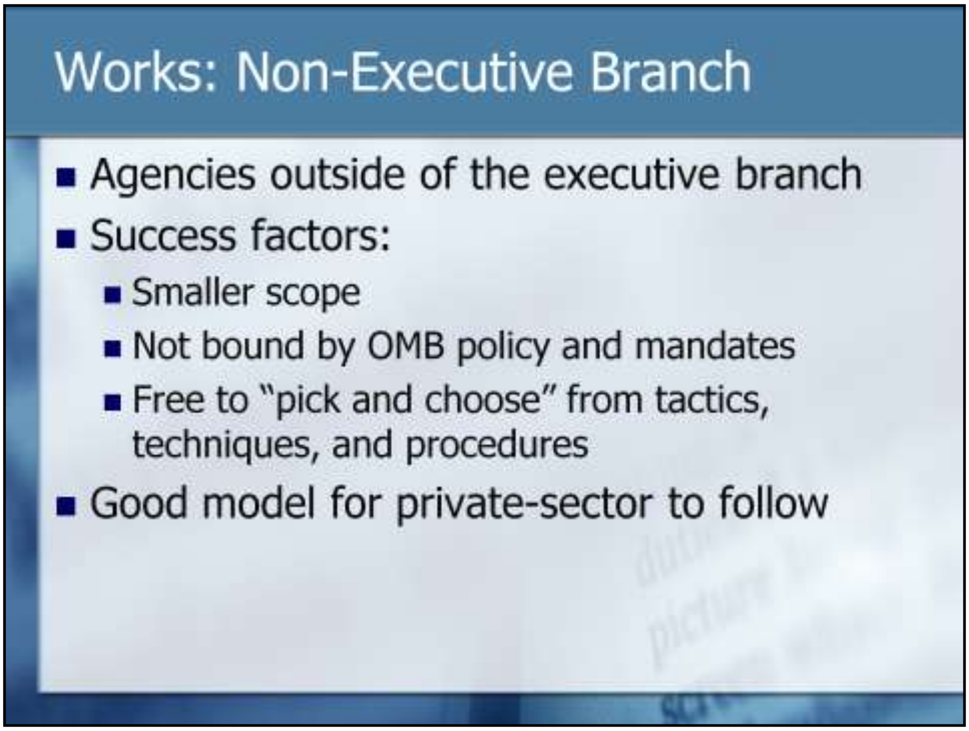
As much as it might seem on the outside that the Government is hyper-focused on the strategic, they actually do produce some very good technical guidance.

STIGs are Security Technical Implementation Guides and they encompass hardening guides and additional system-specific configurations.

http://iase.disa.mil/stigs/stig/index.html

While NIST SP 800-53 is a catalog of controls for Government IT systems, there is a traceability matrix attached as an appendix which traces requirements back to other frameworks such as SOX Section 404 and BS7799.

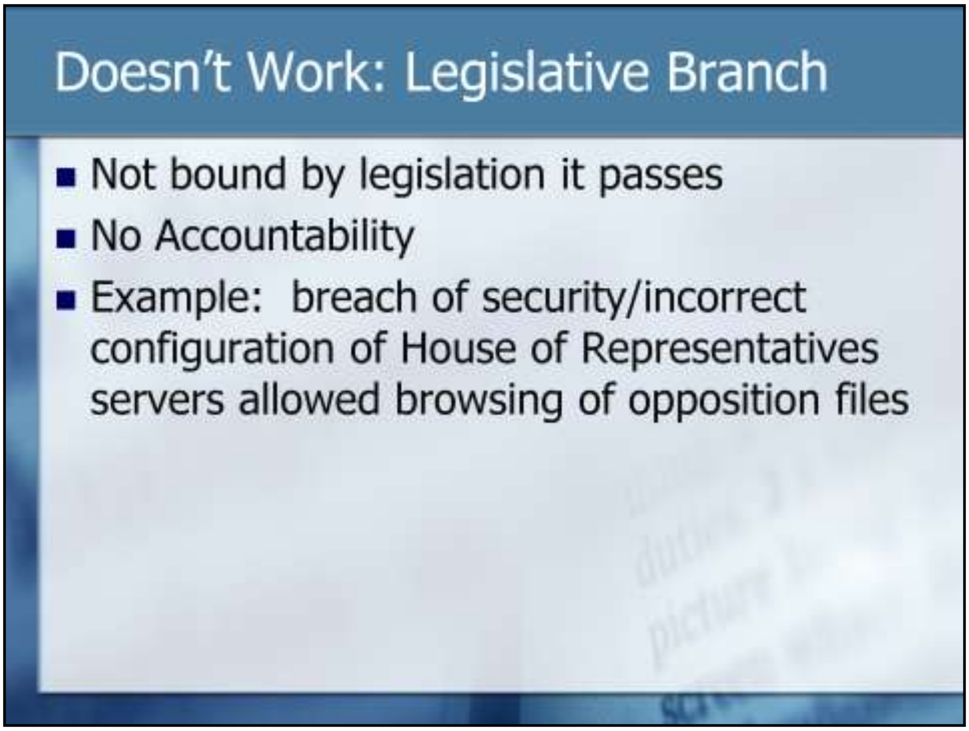
At the strategic level, we have the NIST RMF, elements of which are incorporated in most security SDLCs and risk assessment methodologies.



Works: Non-Executive Branch

- Agencies outside of the executive branch
- Success factors:
  - Smaller scope
  - Not bound by OMB policy and mandates
  - Free to “pick and choose” from tactics, techniques, and procedures
- Good model for private-sector to follow

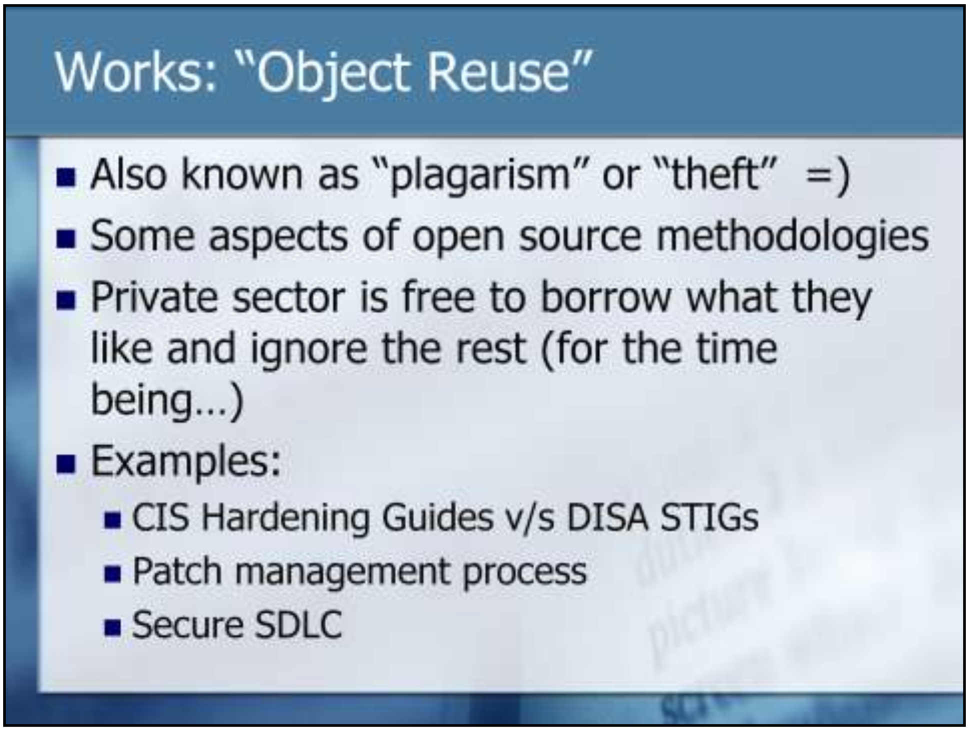
Organizations outside of the Executive Branch have the most leeway on how they secure their data because they are not under the microscope of public scrutiny. As a result, they can select the “best of breed” techniques from the framework and ignore techniques that they deem wasteful.



Doesn’t Work: Legislative Branch

- Not bound by legislation it passes
- No Accountability
- Example: breach of security/incorrect configuration of House of Representatives servers allowed browsing of opposition files

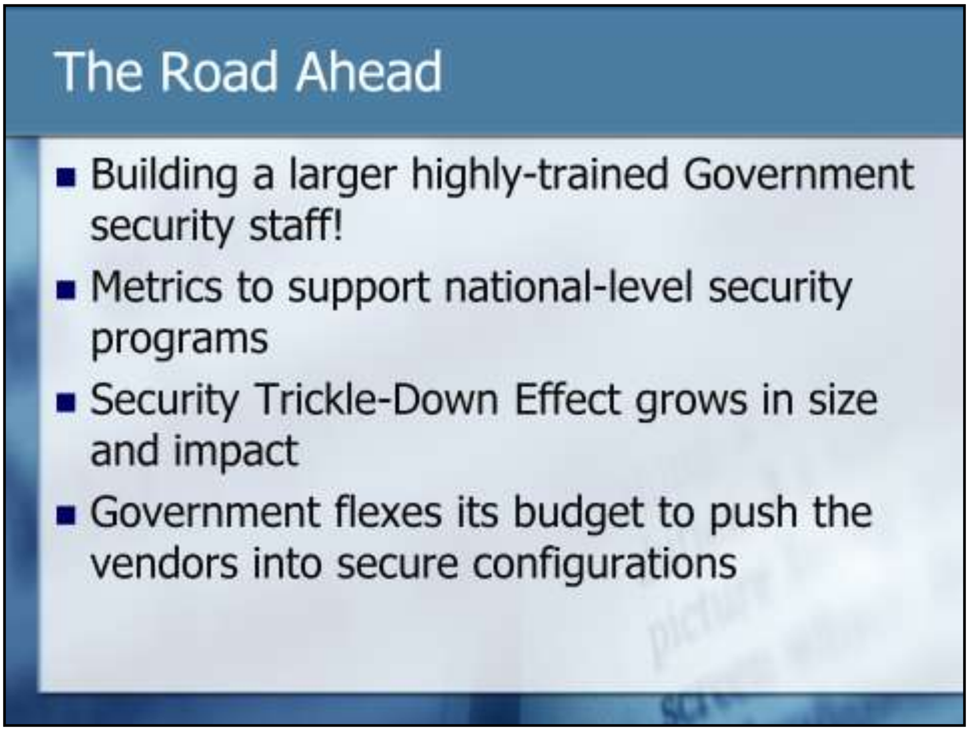
However, sometimes the lack of oversight and audit accountability in the Judicial and Legislative Branches means that they can elect not to choose techniques that they really should.



Works: “Object Reuse”

- Also known as “plagarism” or “theft” =)
- Some aspects of open source methodologies
- Private sector is free to borrow what they like and ignore the rest (for the time being…)
- Examples:
  - CIS Hardening Guides v/s DISA STIGs
  - Patch management process
  - Secure SDLC

The best part about Government techniques, guidance, etc is that they are free for public use. They do not require membership in an organization or royalties.



The Road Ahead

- Building a larger highly-trained Government security staff!
- Metrics to support national-level security programs
- Security Trickle-Down Effect grows in size and impact
- Government flexes its budget to push the vendors into secure configurations

The best thing that you can do for the Government is to help train more security staff. There are many people who have been repurposed from other professions and other compliance-centric governance models who do not understand the basics of risk management.

While the Government does collect metrics, the current set (OMB Memo 07-19) is focused on scope/size of IT assets and how effectively the agencies are complying with the NIST RMF. What the Government needs is a set of metrics to assist in determining national policy.

http://www.guerilla-ciso.com/archives/337

The scope of Government influence in security outside of the beltway will continue to grow as the Government-owned IT assets are secured and we realize that there is more of a dependency on vendors, contractors, and business partners.

Thanks to FDCC, SmartBuy, and other purchasing programs, if the Government decides that they will only purchase IT hardware and software that is secure, it will have an enormous impact on the IT industry.

Questions, Comments, or War Stories?

http://www.guerilla-ciso.com/

rybolov(a)ryzhe.ath.cx

faraonej(a)gmail.com

If you would like us to speak for your event or group, please ask.

If you would like to learn more and to keep up-to-date on groundbreaking Government security news, subscribe to the guerilla-ciso blog feed.