Information Sharing, Security and Privacy – Integration to Improve Programs

Presentation to the ISPAB

October 10, 2012

Dan Chenok, Chair

Information is the Connective Fabric in the 21st Century Economy

- Big data, social media, analytics all allow information sharing in new ways
- Sharing supports stronger program operations, better outcomes, and more knowledge among affected parties
  - Not and end to itself – sharing a means to efficiency and effectiveness across a wide range of public and private sector activity

There are Many Forms of Sharing in the US Government

- Main sharing activity is the Information Sharing Environment in DNI – this is for "terrorism information"
- In addition, info sharing impacts intelligence, homeland security, law enforcement, cybersecurity, as well as many activities of government including:
  - Benefits
  - Enforcement
  - Dissemination

Government has Built Significant Information Sharing Policy and Resources

- Privacy-related laws limit sharing except as authorized by law and/or with adequate notice (and choice in commercial activity)
  - Privacy Act (and Computer Matching Act), HIPAA, GLB, IRS 6103, Statistical Confidentiality laws
- Protection of privacy as a value can restrict the benefits of sharing
  - Supermarket information demonstrates public willingness to make trades – sharing for an outcome, convenience and price reductions
  - Government needs to build trust to support sharing for better outcomes

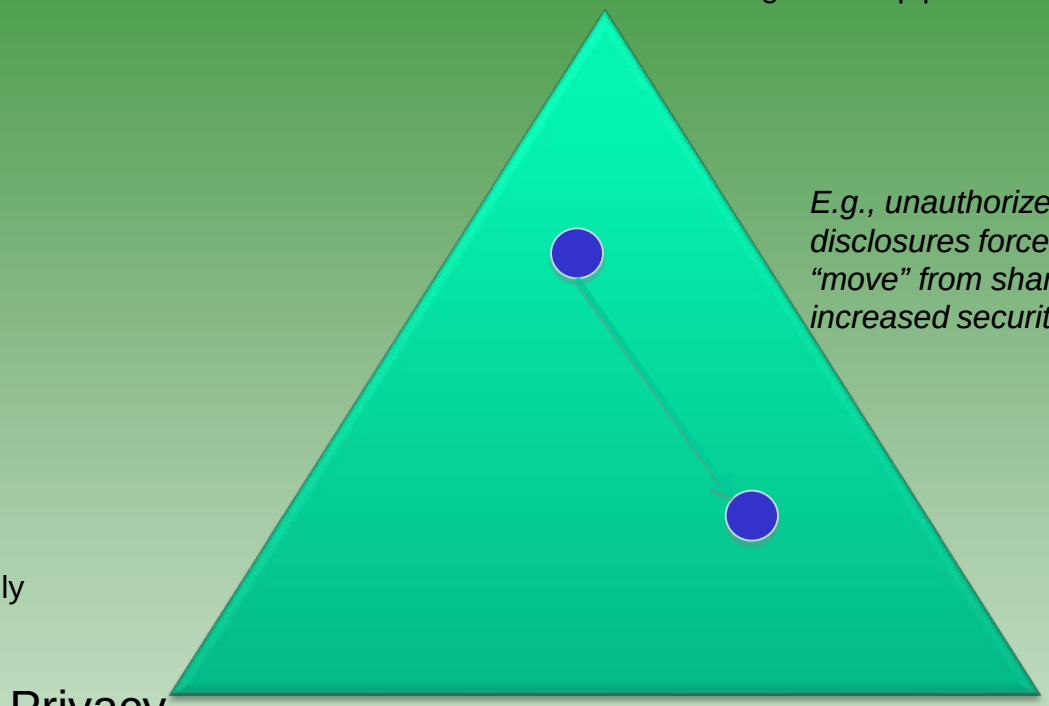
Government has Built Significant Information Sharing Policy and Resources

- Cybersecurity interacts with sharing in two ways:
  - Securing the information that is shared
  - Benefitting from improved sharing about vulnerabilities, threats, and responses
- The latter gets most attention from cyber professionals, but the former has a wider impact on the universe of programs that benefits from sharing
  - Need to secure the information, not the systems
- ISPAB – change from CSSPAB was not accidental
  - So what to do to promote sharing, protect privacy, and provide security?

Info Sharers are not Cyber or Privacy Professionals

- Yet they run or oversee most of the information sharing activities
- Therefore, to be effective at enabling sharing while promoting privacy and security, steps need to clearly reinforce the programs supported by information
  - Build trust from the outset
- Start with the basics
  - Education – this is cyber awareness month, are we reaching managers on a level that explains why cyber protects their mission goals
  - Basic security – make them understand the risks in a simple way
  - Understand need to protect PII to build trust

Move from Balancing to Integration among Sharing, Security, Privacy



respond to calls for increased sharing, fight 'stovepipes'

E.g., unauthorized disclosures force CIOs to "move" from sharing to increased security

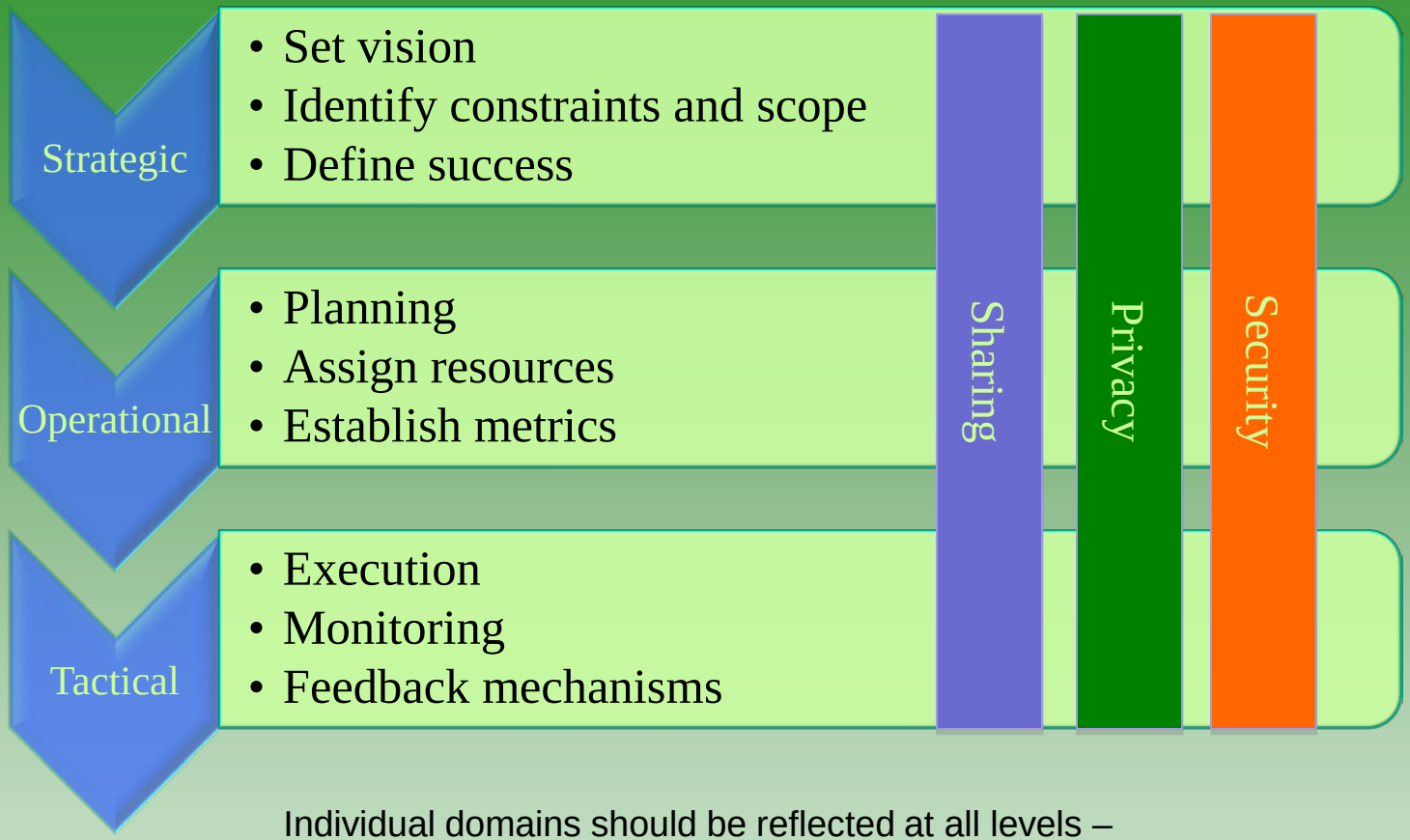
protect Personally Identifiable Information

protect confidential data from unauthorized access

Many government and commercial entities believe they must strike a balance among privacy, security and sharing for their enterprise data and information.

But this balance may shift based on exogenous events.

Integrating (not balancing) Sharing, Security, Privacy



Individual domains should be reflected at all levels – not just implemented at the Tactical level or dreamed of at the Strategic level

There should be an integrated Sharing, Privacy, and Security strategy

At every level, from grand strategy through execution, principles for sharing, privacy and security must be reflected

Integration Requires A New Set of Framing Questions

From: What are the new security requirements?

To: How do the new security requirements inhibit necessary sharing? What risks can we assume?

From: What can we lock down?

To: What needs to be locked down to protect what is necessary while optimizing what is shared?

From: We should move to social media!

To: How can social media be leveraged to share more effectively? What are the risks and mitigation strategies?

From: What's the strongest password policy?

To: How can sharing be done so as not to place PII at risk?

Privacy to Build Trust– FIPPs-based Principles for Info Sharing

- Risk analysis should inform the level of protection, detection, and mitigation relative to the benefit of sharing
- Protect digital information under consistent rules -- seek court review for access to electronic records
- For PII, ensure proper review where cyber protection requires surveillance consistent with law
- Examine content of messages only in cases of near-term and high risk
- Correct for inaccuracies – destroy information that should not have been tracked via mitigation, don’t share misinformation
- Officials with a privacy interest should be involved in the development of sharing programs
- Notice should go to individuals if information from their machines are causing a problem (WHO model)

Security to Build Trust – New Structures and an Operational Perspective

- Operational security to enable real-time sharing
  - Allows issues to be spotted and corrected early, relative to the compliance mode
- Bring the National Security and Civilian regimes together under a risk-based model
  - Promote sharing across the historical wall
- Move to an information-based model of protection, rather than a system-based model
  - Adapts to cloud, analytics, social media, etc.
  - Policy should distinguish between aggregate and PII

Privacy and Security in this Context – Potential Oversight for Sharing Cyber Information

- Government will share extensive information with industry on the condition that industry agrees to voluntarily comply with strong privacy safeguards
- This should be accompanied by positive incentives for industry to share information with government – if you share in a privacy-enhancing manner, safe harbors could accrue
- Central leadership for policy and lead on large issues, with individual agencies handling small issues based on centrally issued policy.
- The central group must be independent to ensure adherence to law and policy, separate from but representative of implementing agencies, industry, and the advocacy community
  - Issue policy
  - Oversee audit and compliance activity
- Key oversight criteria is whether the sharing program provides both benefit and protection

Two Challenges Impacting Government

- **Redisclosure** – how do I trust that you won't re-release?
  - Technical solutions – prevent copying of received data, build systems based on access not sharing
  - Policy incentives – if you redisclose, funding is in jeopardy, if serious could have stronger measures (legal, admin)

- **"Open Sharing" Increases Focus on Integrating Privacy and Security**
  - Law Enforcement, intelligence traditionally done over protected systems
  - Sharing and Analysis of open source data is a key addition to the closed system approach
    - Systems used to do web-based collection and sharing are by nature easy targets

Challenges and Strategies, cont.

- **Proper authentication**
  - Identity and access management frameworks are critical to establishing trusted, assured, identity -- foundational to information sharing and protection.
  - Continue to harmonize identity, credentials and access management frameworks.
  - NSTIC's ecosystem approach is an opportunity to build from

More to Come

- CSIS Paper
- DPIAC Report