VA INFORMATION PROTECTION

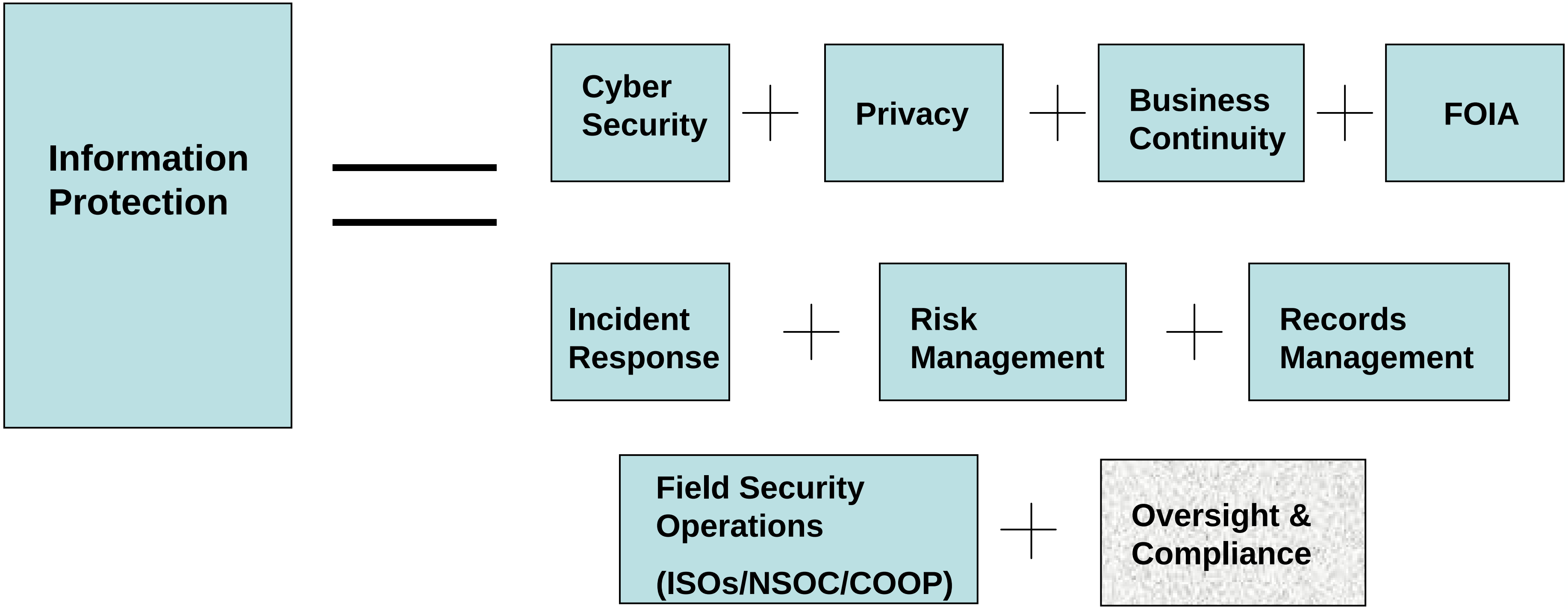
Department of Veterans Affairs

Privacy: The Key to a Successful Information Protection Program

K. Adair Martinez
Deputy Assistant Secretary
Information Protection & Risk Management
March 2008

VA Information Protection Vision

“To Achieve the Gold Standard in Information Protection”



Information Protection

=

Cyber Security + Privacy + Business Continuity + FOIA

Incident Response + Risk Management + Records Management

Field Security Operations (ISOs/NSOC/COOP) + Oversight & Compliance

Discussion

- *Privacy: Why It Is so Important*
- *Privacy Assessment & Recommendations*
- *Innovative Training and Awareness Activities*
- *Conclusions/Questions*

What Is Privacy?

Privacy is Essential to Security

THERE CAN BE <u>NO PRIVACY</u> WITHOUT SECURITY. PRIVACY IS ENSURED IN PART BY SECURITY CONTROLS!

Privacy is WHAT we Protect

Security is HOW we Protect it

VA Information Protection Program:
Protecting PII is our #1 Priority

Privacy Requirements

- ***Privacy Act of 1974***
- ***E-Government Act of 2002***
- ***Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule***
- ***Title 38 U.S.C. 5701***
- ***Title 38 U.S.C. 5705***
- ***Title 38 U.S.C. 7332***
- ***Freedom of Information Act of 1966***
- ***Computer Matching and Privacy Protection Act of1988***
- ***Gramm-Leach-Bliley Act of 1999***
- ***Clinger-Cohen Act of 1996***
- ***Paperwork Reduction Act of 1995***
- ***OMB Memo 06-15***
- ***OMB Memo 07-16***
- ***Children's Online Privacy Protection Act of 1998***

*This list may not be all-inclusive.

What Information Should be Protected?

- ***Any information that is paired with:***
  - ***An individual’s name or***
  - ***Other information that can identify an individual***
    - ***SSN, Address, Phone Number, or other unique number or identifier associated with or assigned to an individual***
    - ***Any other information that can be used to reasonably identify an individual***

- ***Any information that can be used to perpetrate ID Theft or Fraud***
  - ***SSN, Date of Birth (DOB), any account number***
- ***Any information that could cause embarrassment or harm to an individual***

What Specific Information Should be Protected?

- ***Any information from a Privacy Act System of Records***
- ***Any Protected Health Information (PHI)***
  - ***Information relating to the past or future medical treatment of an individual***
  - ***Name, contact information and other information found in a medical record***
- ***Any information related to Substance Abuse, HIV and Sickle Cell Anemia***
- ***Any files, records, reports, and other papers and documents pertaining to any claim and the names and addresses of present or former members of the Armed Forces, and their dependents***
- ***Records and documents created by the Department as part of a medical quality-assurance program***
- ***Any VA sensitive information***

VA Privacy Assessment Highlights

- ***Employees have a high level of awareness about privacy; awareness has increased since the May 2006 breach***
- ***There needs to be a balance --efforts to support privacy must be comparable to the risk, focusing on privacy should not adversely affect their ability to do their jobs***
- ***Training continues to be the most effective way to inform employees about privacy***

Communications Recommendations

- *Stagger distribution of privacy materials so that privacy stays at the forefront of people's minds*
- *Continue to develop and distribute a variety of products because a broad range of products will reach the most people*
- *Provide more guidance/clear rules on release of information – a check list of dos and don'ts*
- *Consider developing multiple brochures for employees and veterans, with different levels of content and various formats*
- *Create a wider variety of posters with different sizes, fonts and styles, each with a simple and specific message.*
  - *Place them in high traffic areas and rotate posters regularly*
- *Provide more information on how to report a privacy incident*

Training Recommendations

- *Stagger the privacy, security and ethics training so issues are reinforced throughout the year*
- *Provide more "real world" examples and scenarios in all of the training.*
- *Update the training each year so it looks and feels different*
- *Strongly urge facilities to consider requiring new staff to take training before they are given access to IT systems*
- *Suggest that Information Security Officers (ISO) should take Privacy Officer training to understand the Privacy Officer's roles and responsibilities*
- *Have all VA training in one place (one website)*
- *Provide different training options and modalities*

Training and Awareness Activities

- ***Newsletters***
- ***Posters***
- ***Information Protection Week***
- ***Satellite Broadcasts***
- ***InfoSec Conference***
- ***Privacy Training***
- ***Security Training***

Lessons Learned

- ***Establish good working relationship with the Privacy Officer and the Information Security Officer (ISO) to coordinate privacy and security activities such as documenting and reporting privacy/security violations***

- ***Promote activities to foster privacy/security awareness, e.g. Privacy/Security Day***

- ***Coordinate meetings to share privacy/security issues regarding protecting (PII)***

- ***Work closely with VA Stakeholders to communicate privacy/security gaps within VA policies***

Conclusions/Questions

- *Privacy is what we protect*
- *Security is how we protect it*
- *Focus on the Information – the Real Value*
- *Losing ones identity – an extreme crisis, we cannot contribute to this in any way*
- *Must create a ‘culture of security’*
- *Deter, Detect and Defend*
- *Eliminate the Use of SSNs*
- *Golden Rule for PII*

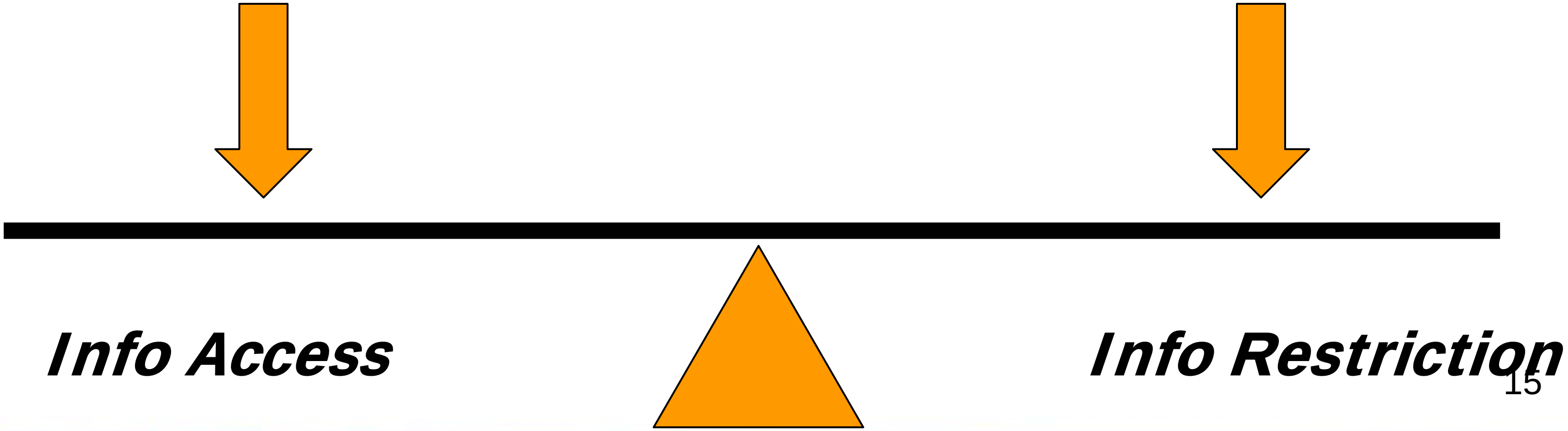
Cyber security and privacy are only as strong as the weakest link in the chain of information protection

Balancing Act

Finding the Right Balance!

- Clinical Care
- Research collaborations
- Training Programs
- Quality improvement

- Federal law
- Congress
- OMB
- Veterans groups
- Public distrust
- Litigation



Info Access

Info Restriction