A Structured Approach for Privacy Risk Assessments for Federal Organizations

Dr. Sarbari Gupta

President and CEO, Electrosoft

NIST Cybersecurity Risk Management Conference

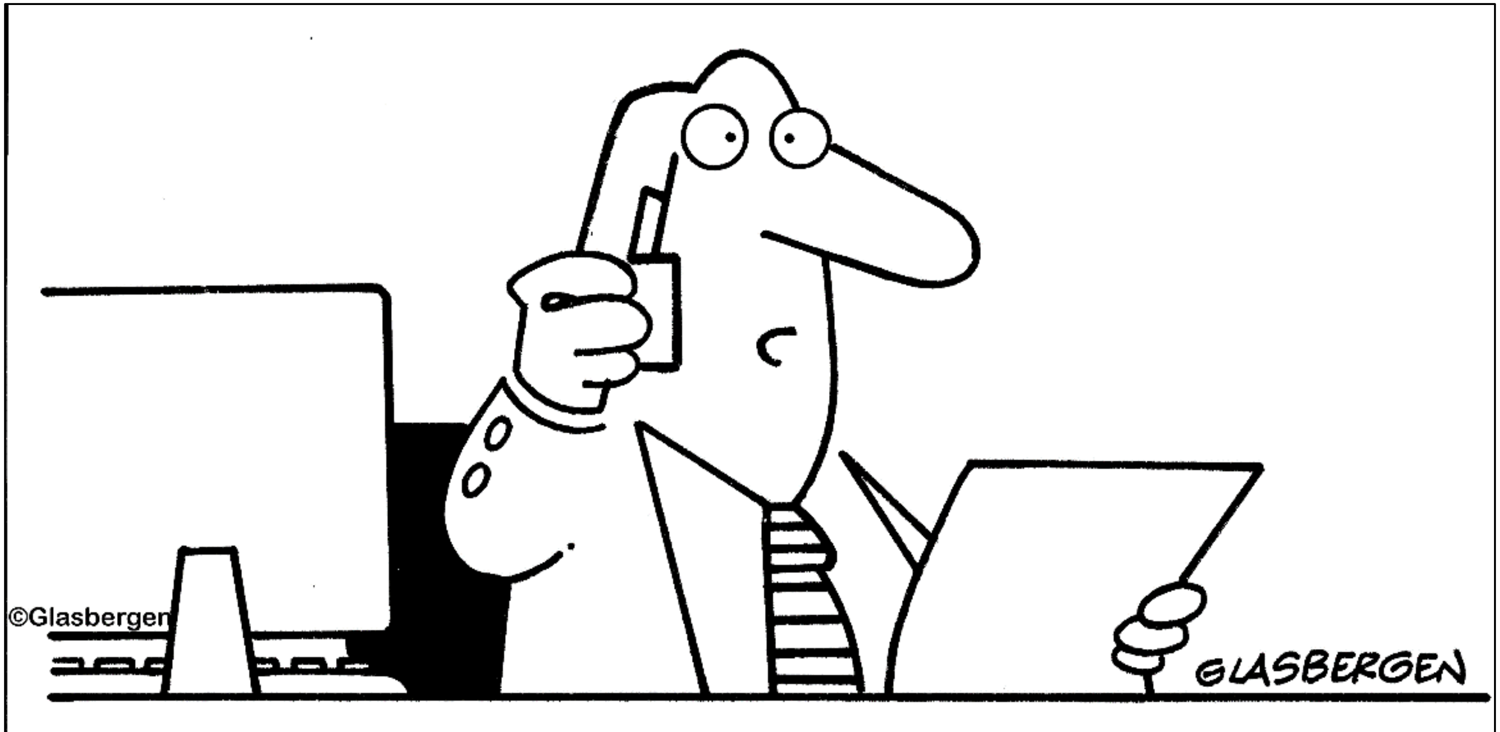
November 7-9, 2018

Baltimore, MD

Electrosoft Services, Inc.
1893 Metro Center Drive
Suite 228
Reston, VA 20190

Web: http://www.electrosoft-inc.com
Email: info@electrosoft-inc.com
Tel: (703) 437-9451
FAX: (703) 437-9452

Privacy is confusing…



"I sent my bank details and Social Security number in an e-mail, but I put 'PRIVATE FINANCIAL INFO' in the subject line so it should be safe."

Privacy Risk is Real!

- **Impersonation**

Due to Congress's failure to pass legislation to fund the government, the information on this web site may not be up to date. Some submissions may not be processed, and we may not be able to respond to your inquiries.

Use stolen/aggregated personal information to recover account password

Privacy Risk is Real!

- **Spear Phishing using personal information**

"This is an urgent message from Lieb School. Your daughter Chrissy had a sudden accident. Please call this number immediately!"

Privacy Risk is Real!

- **Attack on Credibility/Viability of Company**

ICD 10 Code
Certain infectious and parasitic diseases (A00
Intestinal infectious diseases (A00-A09)
A00 Cholera
A01 Typhoid and paratyphoid fevers
A02 Other salmonella infections
A03 Shigellosis
A04 Other bacterial intestinal infections
A05 Other bacterial foodborne intoxications
A06 Amoebiasis
A07 Other protozoal intestinal diseases
A08 Viral and other specified intestinal infectio
A09 Diarrhoea and gastroenteritis of presume
Tuberculosis (A15-A19)
A15 Respiratory tuberculosis, bacteriologically
A16 Respiratory tuberculosis, not confirmed b
A17 Tuberculosis of nervous system
A18 Tuberculosis of other organs
A19 Miliary tuberculosis
Certain zoonotic bacterial diseases (A20-A28
A20 Plague
A21 Tularaemia
A22 Anthrax
A23 Brucellosis
A24 Glanders and melioidosis
A25 Rat-bite fevers
A26 Erysipeloid
A27 Leptospirosis
A28 Other zoonotic bacterial diseases, not els
Other bacterial diseases (A30-A49)
A30 Leprosy [Hansen's disease]
A31 Infection due to other mycobacteria
A32 Listeriosis
Electronic Medical Record System
Home
Show
Print
Send
Preview
Edit
Save
Quit
Personal Information
Social Information
Insurance
Diagnosis
Treatment
Medical History
Healthcare Calendar
Schedule
Appointment
HN:
Patient Name:
Doctor
Operative Note :
Search ● HN ○ Name ○ Doctor
Search
Personal Information

Steal health records about CEO's terminal illness

Leak CEO health status to the press to tarnish credibility/viability of company

Examples of Privacy Attacks

- **Using Personally Identifiable Information (PII) to:**
  - ***Impersonate an individual and obtain unauthorized access/services***
  - ***Cause or threaten physical harm to the individual (e.g. burglary, stalking, blackmail, physical attack)***
  - ***Attack reputation/stature/credibility of an individual***
  - ***Make a political statement***
  - ***Conduct spear phishing***
  - ***Conduct targeted marketing***

Privacy and Federal Government

- Federal Agencies need to collect, use and disseminate PII to achieve their mission

- Federal Regulations/Statutes to protect privacy of individuals
  - ***Privacy Act of 1974***
  - ***Section 208 of E-Government Act of 2002***
  - ***OMB Memos …***

OMB M-03-22 Guidance on Section 208 of E-Gov Act of 2002

- **Requirements for Agencies**
  - ***Conduct privacy impact assessments* for electronic information systems and … make them publicly available**
  - ***Post privacy policies on agency websites and … translate … into a standardized machine-readable format***
  - ***Report annually to OMB on compliance with section 208 of the E-Government Act of 2002***
- **Definitions**
  - ***Privacy Impact Assessments (PIA) - an analysis of how information is handled:***
    - **To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy**
    - **To determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system**
    - **To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.**

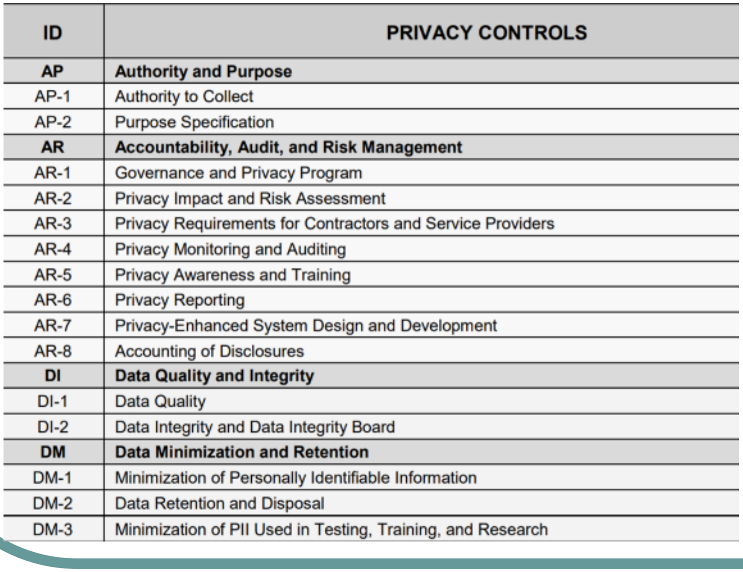
OMB M-03-22 PIA Approach

- **Content**
  - ***What information is to be collected***
  - ***Why the information is being collected***
  - ***Intended use of the information***
  - ***With whom the information will be shared***
  - ***What opportunities individuals have to control particular uses of the information***
  - ***How the information will be secured***
  - ***whether a system of records is being created under the Privacy Act***
- **Analysis**
  - ***Address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified above***

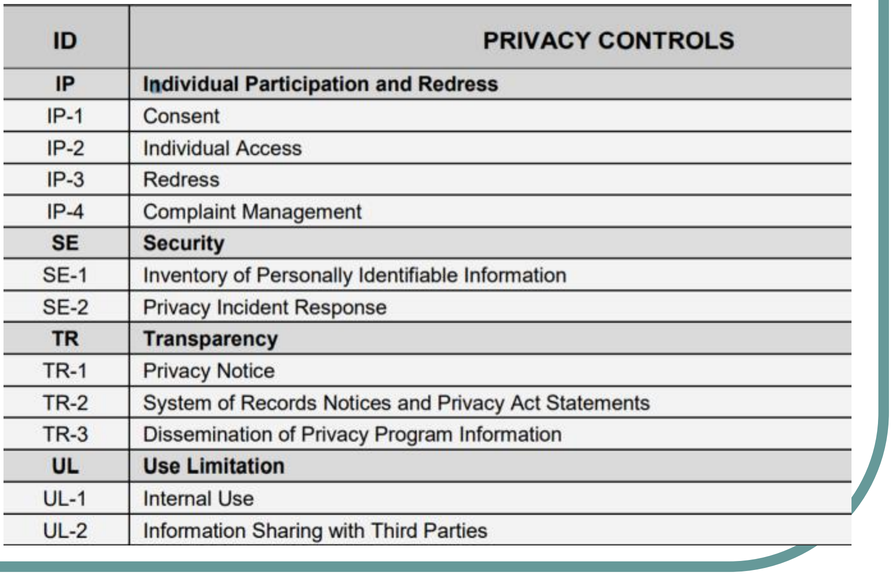
Challenge:
Not easy to assess impact and identify risk to individuals

NIST SP 800-53 r4 Privacy Control Catalog

- **Structured set of privacy controls (organized under eight families)**
- **Unlike security controls, privacy controls are NOT allocated to the low, moderate, and high baselines.**
  - ***Agencies are expected to select and implement controls based on the applicable privacy requirements***



ID	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research



ID	PRIVACY CONTROLS
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

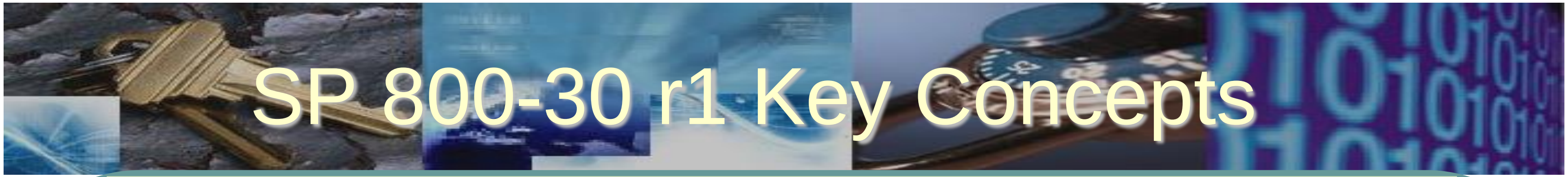
AR-2 Calls for Privacy Risk Assessments

- **AR-2 Privacy Impact and Risk Assessment - The organization:**
  - ***a. Documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and***
  - ***b. Conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.***

How to Conduct a Privacy Risk Assessment?

- **Privacy Risks versus Security Risks**
  - ***Security risks – directed at Organizations and Information Systems/Assets***
  - ***Privacy Risks – directed primarily at Individuals***
- **Privacy Threats and Risks**
  - ***Not well articulated in Federal policy or guidelines***
- **Privacy Risk Assessment**
  - ***No structured approach proposed in Federal policy or guidance***

Risks?



SP 800-30 r1 Key Concepts

- Risk assessment - The process of identifying, estimating, and prioritizing … risks
- Risk - A measure of the extent to which an entity is threatened by a potential circumstance or event
- Threat – Any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation
- Vulnerability – A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source
- Level of Impact – The magnitude of harm that can be expected to result from a threat event
- Likelihood of Occurrence – A weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities)

SP 800-30 r1 Risk Assessment Methodology (adapted for PRA)

- **Consider:**
  - ***Relevant privacy Threats to individuals and organizations;***
  - ***Vulnerabilities both internal and external to organizations that can result in risk for individuals;***
  - ***Impact (i.e., harm) to individuals and organizations that may occur given the potential for threats exploiting vulnerabilities; and***
  - ***Likelihood that harm will occur***
- **Determine risk (as function of the degree of harm and likelihood of harm occurring)**
- **Categorize risks**

**** Underlined words indicate adaptations for PRA***

What is Privacy Risk?

- **Privacy Risk - Risk to the individual and organizations when PII handled by an organization or organizational information system suffers from:**
  - ***Unauthorized collection, use, sharing and retention***
  - ***Absent or Insufficient notification to the individual on scope and purpose***
  - ***Low quality or inaccuracies***
  - ***Unintended aggregation and data mining***
  - ***Unauthorized disclosure***
  - ***Unauthorized modification or destruction***

Privacy Risk Assessment (PRA) – Proposed Approach

- **PRA at Organizational Level (Tier 1)**
  - ***Identifies and categorizes risks to the privacy of individuals that can best be mitigated at the organizational level***
- **PRA at Information System Level (Tier 3)**
  - ***Identifies and categorizes risks to the privacy of individuals that can best be addressed by an information system that handles PII***

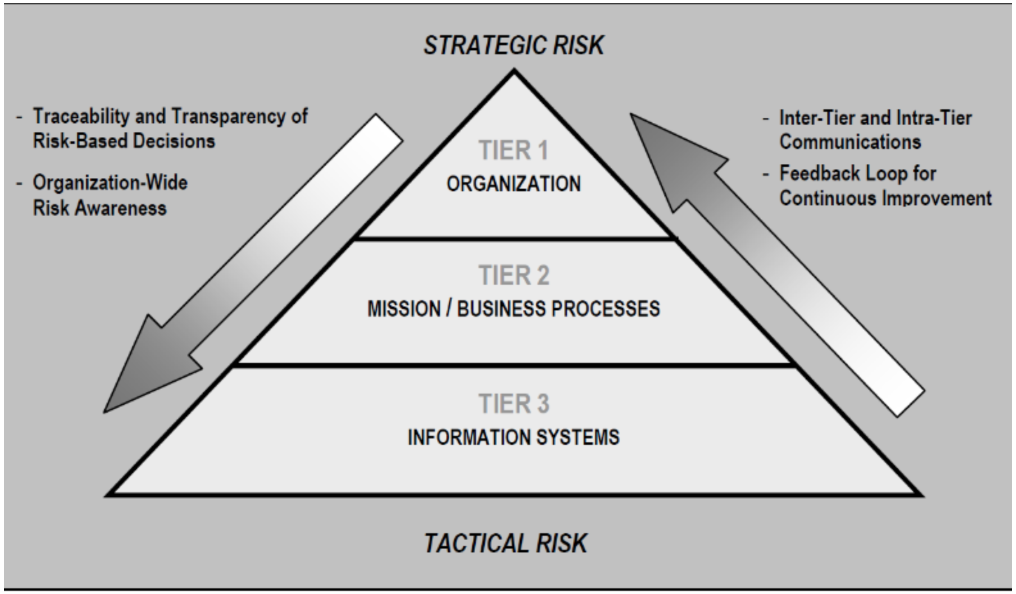

STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

FIGURE 4: RISK MANAGEMENT HIERARCHY

(From SP 800-30 r1)

Privacy Threats at Organization Level

- Collection/use of PII without proper authority
- Ineffective or absent privacy notices (PTAs/PIAs/SORNs#)
- Agency Information Systems handle PII in risky manner
- Contractors/ Service Providers handle PII in risky manner
- Agency personnel unware of privacy mandates and associated risks
- Quality of PII collected/used is suspect
- Privacy program information is not available to public
- Individuals do not have a way to complain about privacy practices

Threats related to Governance, Policies, Procedures, Templates, Training, etc.

# PTA – Privacy Threshold Analysis; SORN – System of Record Notice

Privacy Threats at Information System Level

- Collection/Distribution of inaccurate or low quality personal information by Agency
- Agency Insiders who leak personal information
- Spear Phishing through Personal Data Aggregation / Inference
- Cyber criminals looking for financial gain (through blackmail, extortion, account hacking)
- Attackers intending physical harm (e.g., kidnappers, burglars, stalkers)
- Targeted marketing using aggregated personal information
- Political statements using personal information
- Erosion of organizational or individual reputation / credibility / creditworthiness

Privacy Vulnerabilities - I (weaknesses in implementing SP 800-53 r3 Privacy Controls)

ID	Privacy Controls	Responsibility		Significant Actions
		Org	IS	
AP	**Authority and Purpose**			
AP-1	Authority to Collect		Yes	Documents legal authority for PII collection/use
AP-2	Purpose Specification		Yes	Documents purpose of PII collection/use
AR	**Accountability, Audit, and Risk Management**			
AR-1	Governance and Privacy Program	Yes		Appoints SAOP/CPO Develops Org Privacy Plan Develops/Disseminates Privacy Policies/Procedures
AR-2	Privacy Impact and Risk Assessment	Yes	Yes	Develops process for assessing privacy risk (Org) Conducts PIAs for Information Systems (IS)
AR-3	Privacy Requirements for Contractors and Service Providers	Yes		Includes privacy requirements in contracts
AR-4	Privacy Monitoring and Auditing	Yes		Monitors and audits privacy controls and policy
AR-5	Privacy Awareness and Training	Yes		Provides general and role-based privacy training
AR-6	Privacy Reporting	Yes		Reports to OMB and oversight bodies on privacy compliance
AR-7	Privacy-Enhanced System Design and Development		Yes	Deisgns IS to automate privacy controls
AR-8	Accounting of Disclosures		Yes	Maintains and provides accounting of disclosures

Privacy Vulnerabilities - II (weaknesses in implementing SP 800-53 r3 App J controls)

ID	Privacy Controls	Responsibility		Significant Actions
		Org	IS	
DI	**Data Quality and Integrity**			
DI-1	Data Quality		Yes	Ensures acccuracy/timeliness/completeness of PII
DI-2	Data Integrity and Data Integrity Board	Yes	Yes	Establishes a Data Integrity Board when appropriate (Org) Ensures integrity of PII (IS)
DM	**Data Minimization and Retention**			
DM-1	Minimization of Personally Identifiable Information	Yes	Yes	Conducts regular evaluations of PII holdings (Org) Minimizes collection/retention of PII holdings (IS)
DM-2	Data Retention and Disposal		Yes	Retains and destroys PII in accordance with law
DM-3	Minimization of PII Used in Testing, Training, and Research	Yes	Yes	Develops Policies/Procedures (Org) Protects PII used in testing/training/research (IS)
IP	**Individual Participation and Redress**			
IP-1	Consent		Yes	Allows individuals to authorize PII collection/use
IP-2	Individual Access		Yes	Alows individuals access to their PII
IP-3	Redress		Yes	Allows individuals to correct inaccurate PII
IP-4	Complaint Management	Yes		Receives/responds to complaints about privacy practices

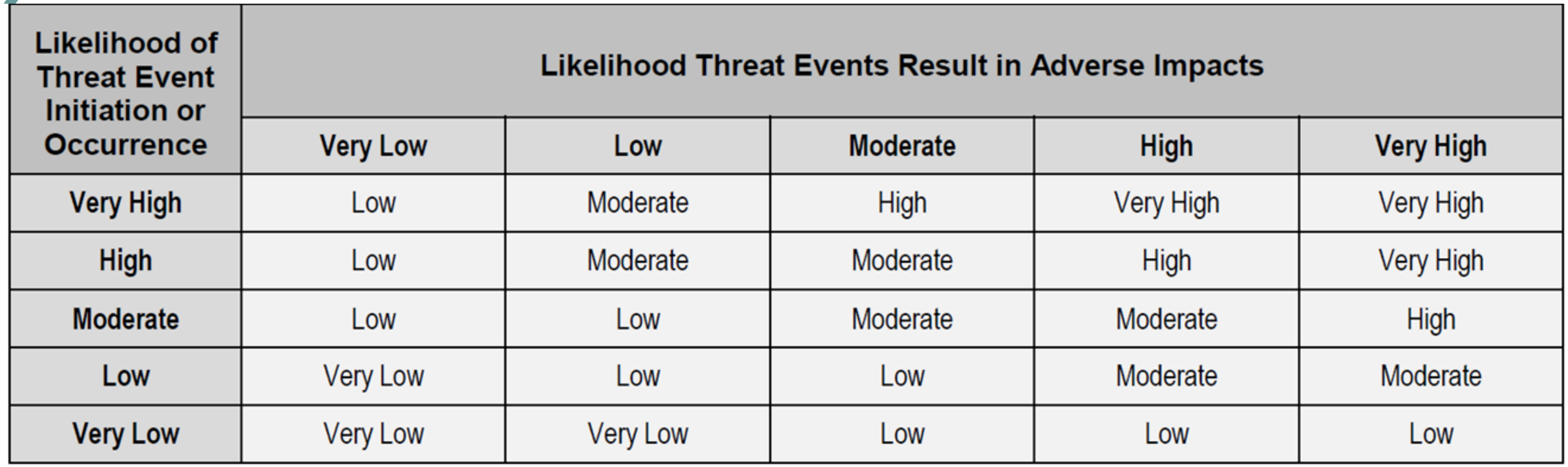
Privacy Vulnerabilities - III (weaknesses in implementing SP 800-53 r3 App J controls)

ID	Privacy Controls	Responsibility		Significant Actions
		Org	IS	
SE	**Security**			
SE-1	Inventory of Personally Identifiable Information	Yes	Yes	Reports PII collection/use by Information Systems to CISO (Org) Maintains inventory of PII collected/used (IS)
SE-2	Privacy Incident Response	Yes		Develops/Implements privacy incident response plan
TR	**Transparency**			
TR-1	Privacy Notice		Yes	Provides notice on privacy activties and PII collection/use
TR-2	System of Records Notices and Privacy Act Statements		Yes	Publishes current SORNs in federal register
TR-3	Dissemination of Privacy Program Information	Yes		Provides access to privacy program activities Ensures SAOP/CPO is accessible to public
UL	**Use Limitation**			
UL-1	Internal Use		Yes	Uses PII internally only for authorized use
UL-2	Information Sharing with Third Parties		Yes	Shares PII externally only as authorized

Examples of Impacts of Threat Events

- **Impact to Individuals**
  - ***Financial loss***
  - ***Physical Harm***
  - ***Damage to Image or Reputation***
  - ***Loss of Creditworthiness***
  - ***Unwanted Targeting/Solicitation***
  - ***Improper delivery of services (such as health services) based on inaccurate or missing PII***
- **Impact to Organizations**
  - ***Erode customer trust or public trust***
  - ***Legal Impacts***
  - ***Financial and Operational Impacts due to non-compliance***

Likelihood and Impact Determination (from SP 800-30 r1)



Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Qualitative Values for Impact of Threat Events	Description
Very High	Multiple severe or catastrophic adverse effects
High	Severe or catastrophic adverse effects
Moderate	Serious adverse effects
Low	Limited adverse effects
Very Low	Negligible adverse effects

Risk Determination and Categorization (from SP 800-30 r1)

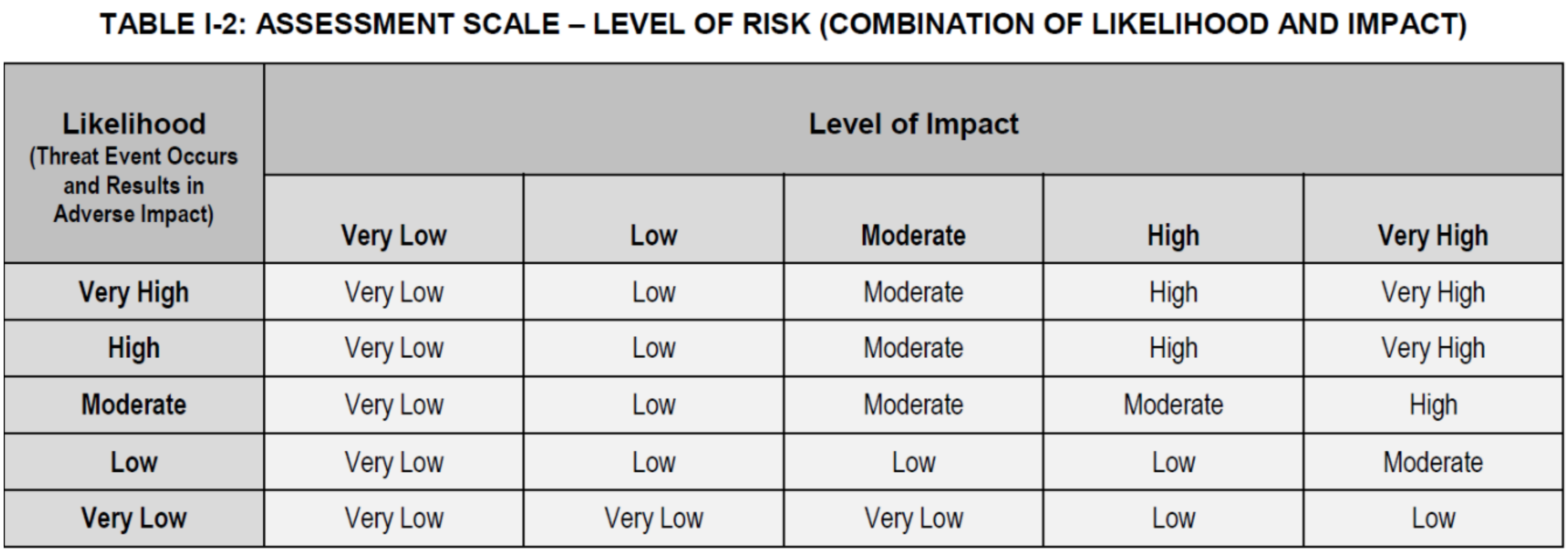


TABLE I-2: ASSESSMENT SCALE – LEVEL OF RISK (COMBINATION OF LIKELIHOOD AND IMPACT)

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

PRA Approach Summary

- **PRAs are essential for compliance and managing privacy risk to individuals**
- **Adapted SP 800-30 r1 process can be used for PRA**
- **Effective PRAs should be conducted at two levels – Organizational and Information System**
- **For each PRA, identify privacy risks by considering:**
  - ***Relevant Privacy Threats***
  - ***Relevant Privacy Vulnerabilities (SP 800-53r4 privacy control weaknesses)***
  - ***Impact of a Successful Attack***
  - ***Likelihood of Occurrence of a Successful Attack***
- **Analyze results of PRAs to categorize privacy risks**
- **Identify ways to mitigate or eliminate risks starting with the highest category risks**

Questions/Comments

Contact & Company Information

- **Contact Info: Dr. Sarbari Gupta – Electrosoft**
  - ***Email: sarbari@electrosoft-inc.com; Phone: 703-437-9451 ext 12***
  - ***LinkedIn: http://www.linkedin.com/profile/view?id=8759633***

- **About Electrosoft**
  - ***We deliver a diversified set of technology-based solutions and services with a deep focus on cybersecurity***
  - ***We co-authored nearly two dozen NIST security publications!***
  - ***Major Customers: Army, DLA, DOC, GSA, Treasury***
  - ***Founded in 2001; Headquartered in Reston, Virginia***
  - ***Socio-economic Certifications: 8(a), SDB, EDWOSB***
  - ***ISO 9001:2015 registered; CMMI Level 3 rated (DEV and SVC)***
  - ***Website: http://www.electrosoft-inc.com***