Privacy as the Foundation of All We Do in State Government

Cherie Givens, Chief Privacy Officer
October 5, 2022

NCDIT
NORTH CAROLINA
DEPARTMENT OF
INFORMATION
TECHNOLOGY

State Agencies and Citizen/Resident Data

- State agencies hold enormous amounts of data about North Carolinians.
- Duty of care – state adoption of the Fair Information Practice Principles.

1. Transparency
2. Individual Participation
3. Purpose Specification
4. Data Minimization
5. Use Limitation
6. Data Quality and Integrity
7. Security
8. Accountability and Auditing

NCDIT FIPPS: https://it.nc.gov/programs/privacy-data-protection/fair-information-practice-principles
Adapted from Teufel, H. (2008, December 29) The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security [Memorandum]. Department of Homeland Security.

Privacy Awareness and Integration

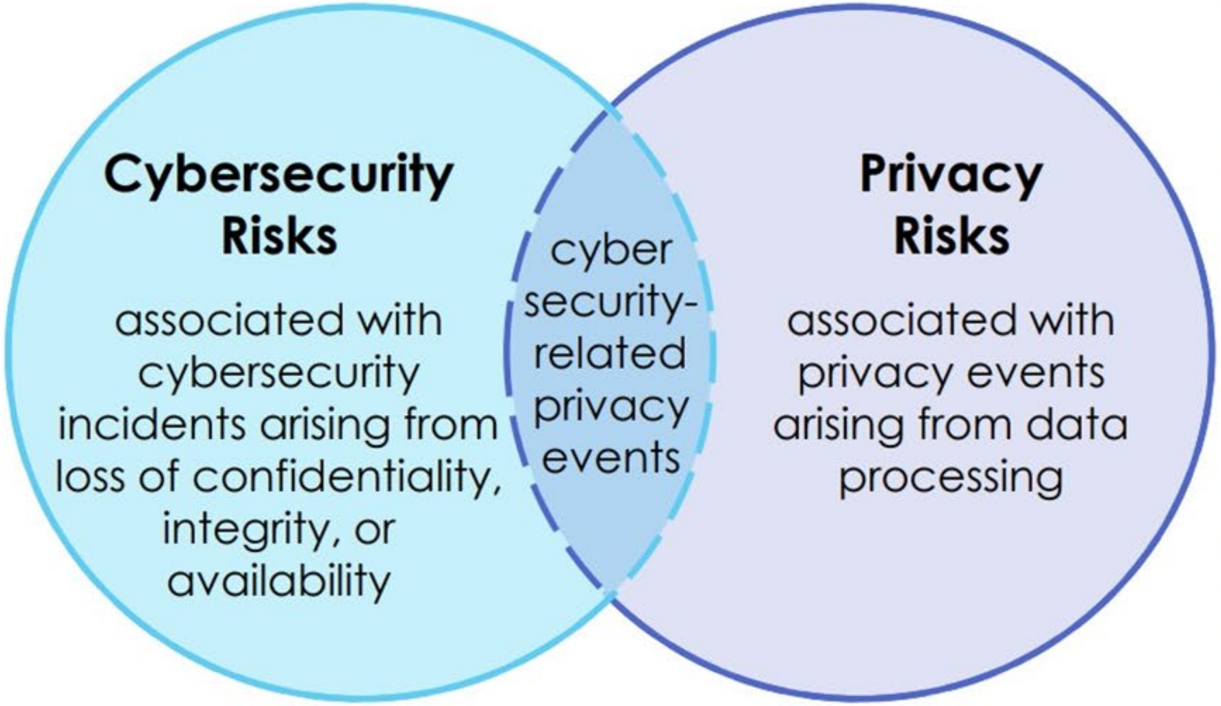
- It is everyone’s responsibility.
- Privacy is more than compliance.
- Privacy is interdisciplinary.
- Privacy should be embedded.
- Privacy should have a seat at the table.

Privacy by Design (PbD)

- Proactive not reactive; preventative not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality – positive-sum, not zero-sum
- End-to-end security – full lifecycle protection
- Visibility and transparency – keep it open
- Respect for user privacy – keep it user-centric

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Relationship Between Cybersecurity and Privacy Risks



Cybersecurity Risks

associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability

cyber security-related privacy events

Privacy Risks

associated with privacy events arising from data processing

NIST, Privacy Framework Presentation, December 2019

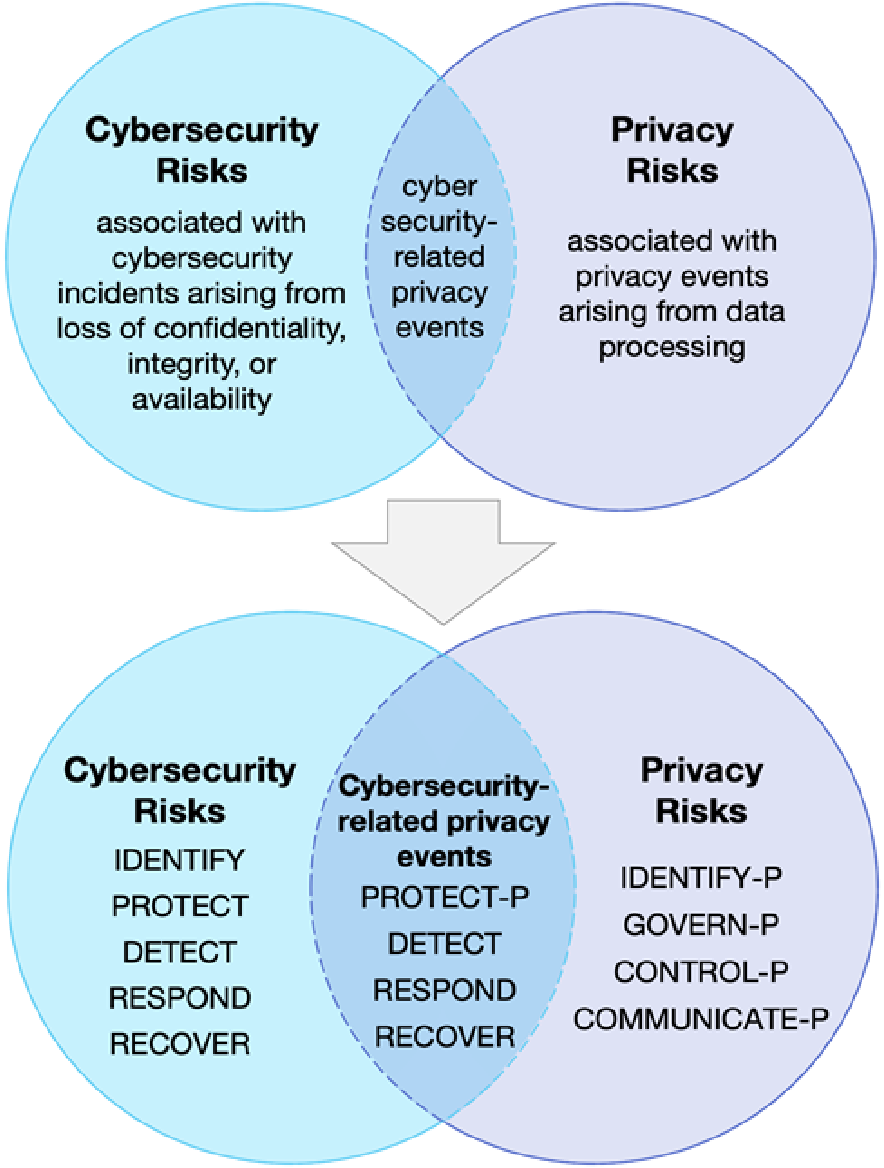
Data: A representation of information, including digital and non-digital formats

Privacy Event: The occurrence or potential occurrence of problematic data actions.

Data Processing: The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal).

Privacy Risk: The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur

NIST Cybersecurity & Privacy Overlap of Controls and Frameworks



Cybersecurity Risks

associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability

cyber security-related privacy events

Privacy Risks

associated with privacy events arising from data processing

Cybersecurity Risks

IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

Cybersecurity-related privacy events

PROTECT-P
DETECT
RESPOND
RECOVER

Privacy Risks

IDENTIFY-P
GOVERN-P
CONTROL-P
COMMUNICATE-P

Five Privacy Risk Management Areas

Identify the data you are collecting, using, sharing, storing.

- Inventory and map the data flow – ingest to destruction
- Need to know the data to understand the privacy risks – level of sensitivity, access
- Privacy Risk Assessments can help – risks and mitigations

*See NIST SP 800-53 and NIST Privacy Framework for more guidance

Five Privacy Risk Management Areas

Govern: Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.

*See NIST SP 800-53 and NIST Privacy Framework for more guidance

NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Five Privacy Risk Management Areas

Control: Develop and implement appropriate activities to enable agencies or individuals to manage data with sufficient granularity to manage privacy risks.

Data Processing Policies, Processes, and Procedures (purpose, scope, roles and responsibilities in the data processing ecosystem, and management commitment) consistent with the agency's risk strategy to protect individuals' privacy (NIST SP 800-53, Rev.5).

Data Processing Management: Data are managed consistent with the agency's risk strategy to protect individuals' privacy, increase manageability, and enable the implementation of FIPPs.

*See NIST SP 800-53 and NIST Privacy Framework for more guidance

Five Privacy Risk Management Areas

Communicate: Develop and implement appropriate activities to enable the agency and individuals to have a reliable understanding about how data are processed and associated privacy risks.

Policies, processes, and procedures are maintained and used to increase transparency of the agency's data processing practices and associated privacy risks.

Mechanisms for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place (privacy notices at intake).

*See NIST SP 800-53 and NIST Privacy Framework for more guidance

Five Privacy Risk Management Areas

Protect (Overlapping with Security): Develop and implement appropriate data processing safeguards.

Security and privacy policies, processes, and procedures are maintained and used to manage the protection of data.

Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.

*See NIST SP 800-53 and NIST Privacy Framework for more guidance

Privacy Questions?

Send an email to **ditprivacy@nc.gov**.