CV PRAM TEMPLATE

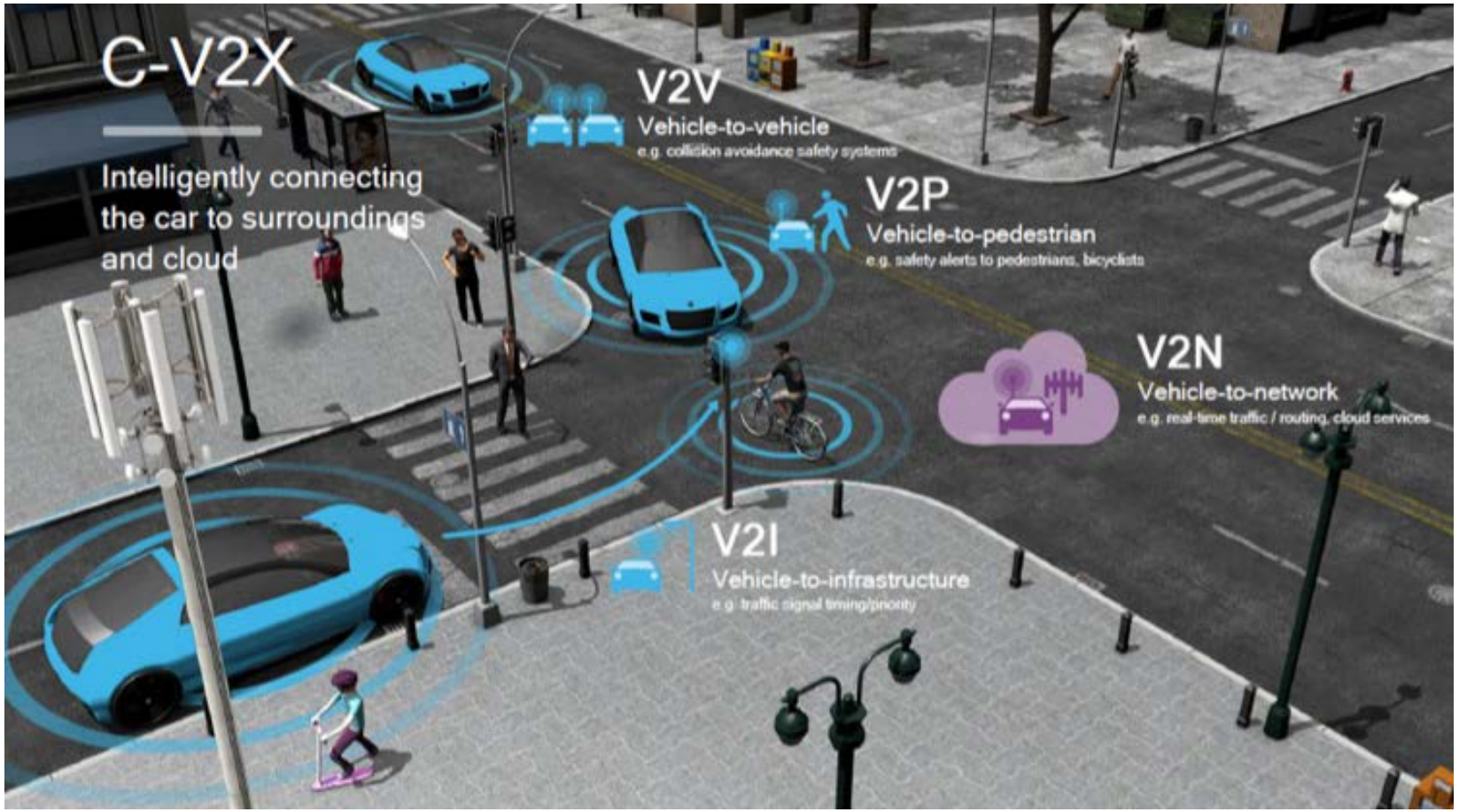
Stuart Shapiro, CIPP/G/US

MITRE

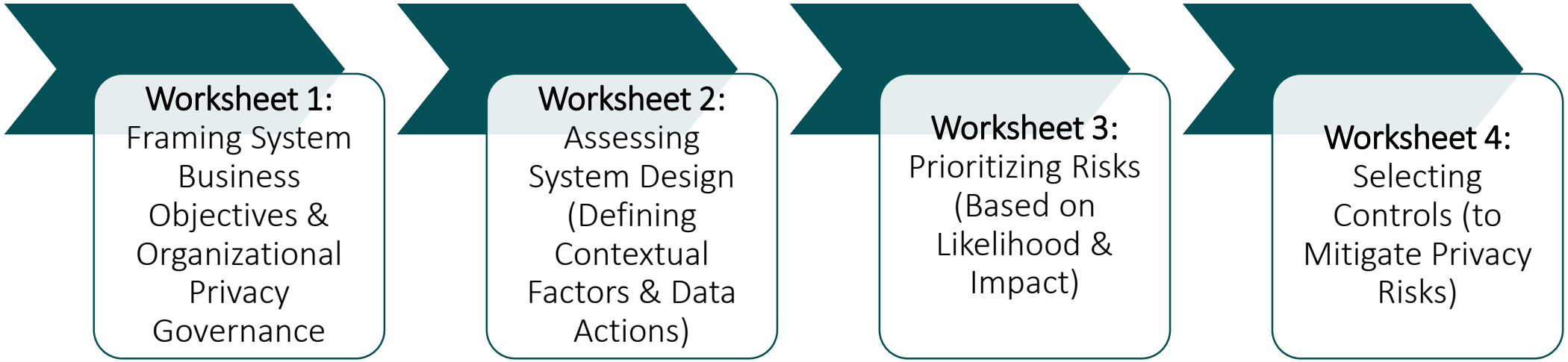
sshapiro@mitre.org

WHY IS PRIVACY AN ISSUE FOR CONNECTED VEHICLES?

- Connectivity!
- Clear text broadcast!
- Identifiers!
- Geolocation!
- Big data!



NIST PRIVACY RISK ASSESSMENT METHODOLOGY (PRAM)



Problematic Data Actions

- Appropriation
- Distortion
- Induced Disclosure
- Insecurity
- Surveillance
- Unanticipated Revelation
- Unwarranted Restriction

Problems for Individuals

- Loss of autonomy
- Exclusion
- Loss of Liberty
- Physical Harm
- Stigmatization
- Power Imbalance
- Loss of Trust
- Economic Loss

Task 1: Frame Business Objectives

1. Describe the functionality of your system(s).
☐ Vehicle/vulnerable road user (VRU)/roadside unit (RSU) device capabilities ☐ Vehicle to vehicle/RSU/backend (direct) communication ☐ VRU to vehicle/RSU/backend (direct) communication ☐ RSU to vehicle/VRU/backend communication ☐ Backend system capabilities ☐ Backend to city/state/federal government/private sector/academia communication

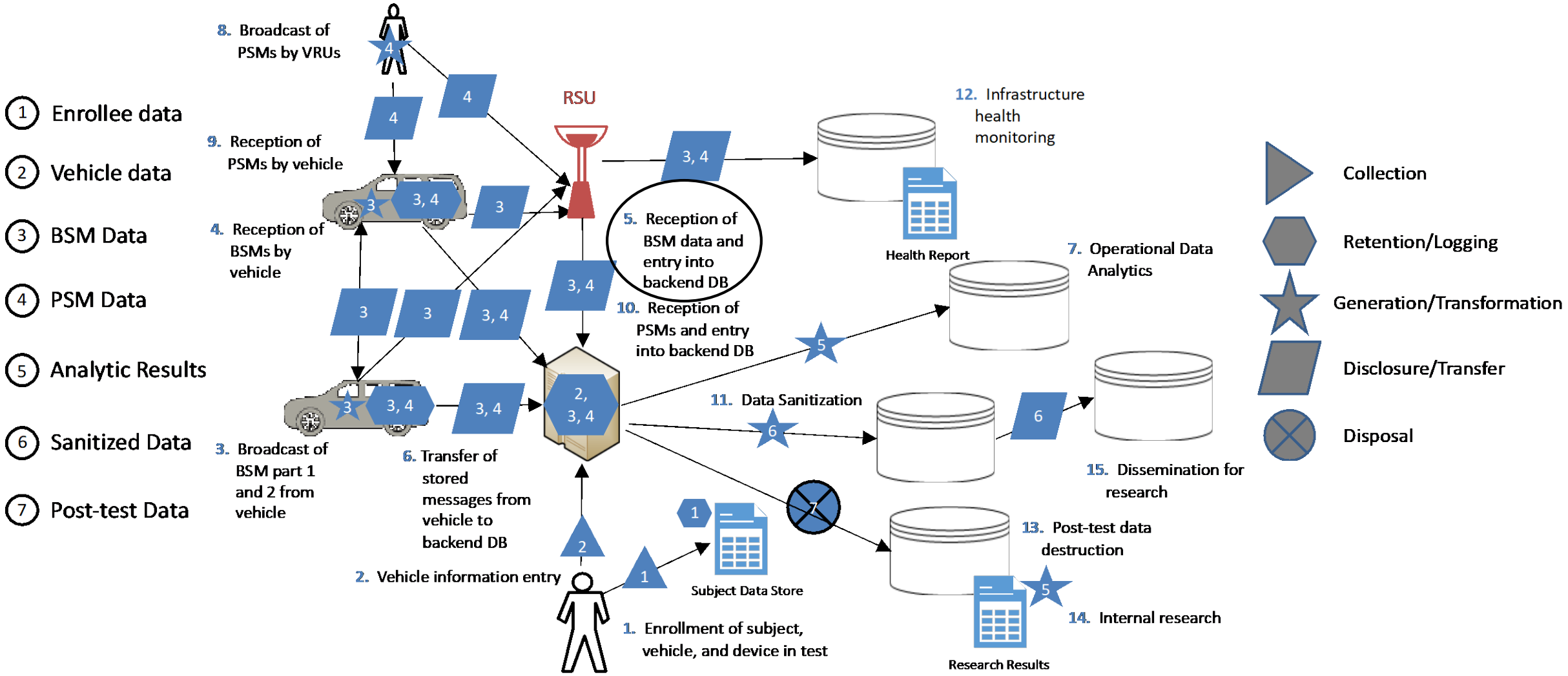
Task 2: Frame Organizational Privacy Governance

1. Legal Environment: Identify any privacy-related statutory, regulatory, contractual and/or other frameworks within which the organization must operate. List any specific privacy requirements.
☐ Contractual privacy and security requirements ☐ Local/state privacy and security statutes and regulations ☐ Common rule for protection of human research subjects   o Institutional Review Board

WORKSHEET 2: CONTEXTUAL FACTORS SELECTED EXAMPLE

Contextual Factors
Organizational
This is human subjects research with a formal IRB approved research protocol governing the study
Relationships between organizations, including municipalities
System
Raw data are available only within the collecting organization
Databases are under the control of the collecting organization
Subject
Potential concern for the data being used against them by law enforcement or by insurer, including, but not limited to, in the event of an accident
Subjects understand that this is research and a unique identifier will tag messages from them

WORKSHEET 2: DATA MAP



WORKSHEET 2: DATA ACTION ANALYSIS SELECTED EXAMPLE

Data Action	Personal Information	Specific Context	[Potential] Summary Issues
DA5: Reception of BSM data and entry into backend database	DeviceID, BSM part 1 and 2 data	As vehicles enter reception range of an RSU, BSMs are received, captured, and offloaded via network infrastructure to a backend server. Data is then entered into a backend database. The database schema limits the specific data that is retained. BSMs from non-participating vehicles may be captured, however, these will not have persistent IDs.	Transmission may be insecure. Unauthorized internal or external use of the DeviceID could allow someone to track the movements of a subject's vehicle and link it to the person by location-based inference. Subjects may not be able to access/remove data from backend database.

WORKSHEET 3: LIKELIHOOD SELECTED EXAMPLE

Data Actions	[Potential] Summary Issues	[Potential] Problematic Data Actions	Potential Problems for Individuals	Likeli-hood
DA5: Reception of BSM data and entry into backend database	Subjects may not be able to access/remove data from backend database.	Unwarranted Restriction	Exclusion (e.g., due to subject inability to remove in whole or in part data pertaining to them)	

WORKSHEET 3: IMPACT

SELECTED EXAMPLE

Data Actions	[Potential] Summary Issues	Problematic Data Actions	Potential Problems for Individuals	Business Impact Factors					Total Business Impact (per Potential Problem)
				Non-compliance Costs	Direct Business Costs	Reputa-tional Costs	Internal Culture Costs	Other	
DA5: Reception of BSM data and entry into backend database	Subjects may not be able to access/remove data from backend database.	Unwarranted Restriction	Exclusion (e.g., due to subject inability to remove in whole or in part data pertaining to them)						

WORKSHEET 3: RISK

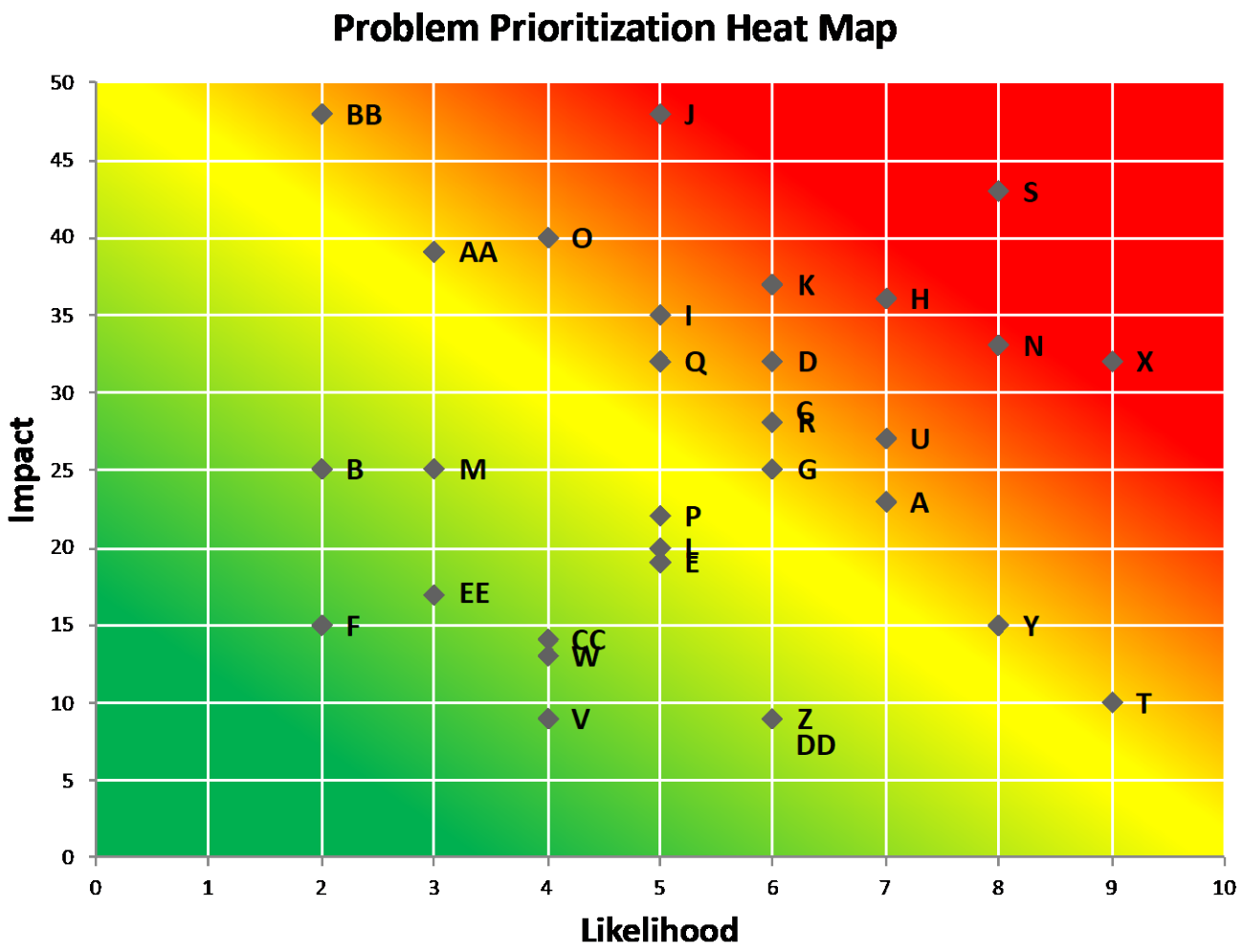
SELECTED EXAMPLE

Data Actions	Potential Problems for Individuals	Likelihood	Business Impact	Risk per Potential Problem	Risk per Data Action
DA5: Reception of BSM data and entry into backend database	Loss of Trust (e.g., due to failure to sufficiently protect information)				0
	Physical Harm (e.g., from being tracked by an abusive partner)				
	Stigmatization (e.g., from being associated with an embarrassing location)				
	Loss of Trust (e.g., due to failure to sufficiently protect information)				
	Economic Loss (e.g., due to criminal targeting of high-value vehicles)				
	Exclusion (e.g., due to subject inability to remove in whole or in part data pertaining to them)				

WORKSHEET 3: RISK PRIORITIZATION

Data Action Risk Prioritization Table

Data Actions	Risk	Percent of System Risk	Rank among Data Actions



WORKSHEET 4: POTENTIAL CONTROLS SELECTED EXAMPLE

Data Actions	Potential Problems for Individuals	[Some] Potential Controls	Considerations
DA5: Reception of BSM data and entry into backend database	Loss of Trust Physical Harm Stigmatization Economic Loss Exclusion	Encrypted backhaul Logical isolation of data (with other message data) Role-based access controls Encryption at rest Enable deletion by subjects during pilot (if persistent ID used)	

WORKSHEET 4: SELECTED CONTROLS SELECTED EXAMPLE

Data Actions	Potential Problems for Individuals	Selected Controls	Rationale	Residual Risks
DA5: Reception of BSM data and entry into backend database	Loss of Trust	*Specific controls chosen for implementation from the set of potential controls*		
	Physical Harm			
	Stigmatization			
	Economic Loss			
	Exclusion			

SOME KEY ISSUES

- Persistent identifiers
- Access and auditing
- Data sanitization

However, every deployment is unique