

Application Implementations with Personally Identifiable Information (PII) Protection

Cyber Risk Analytics and Measurement Program
February 27, 2024

Outline

- Cyber Risk Analytics and Measurement Program
- Personally Identifiable Information (PII)
- Design Considerations
- Application Sample
 - Implementations
 - Secure data handling
- Contact information

Cyber Risk Analytics and Measurement Program

Explore solutions to facilitate the advancement of cybersecurity risk analytics and improve risk management practices

Active projects

- Cybersecurity Measurement
- Cyber Incident Data Analysis
- Cyber Supply Chain Analysis

Personally Identifiable Information (PII)

Definition:

Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

NIST SP 800-53 Rev.5

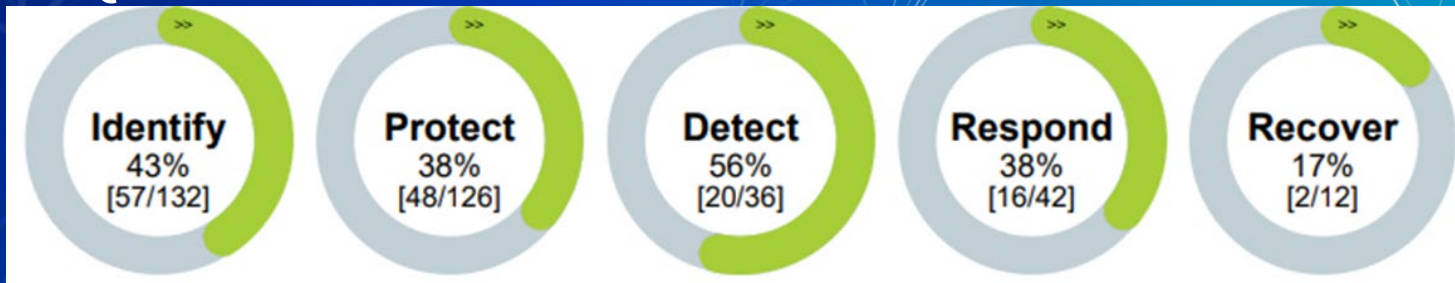
Design Considerations

- PII considerations included in application design from the start
- Apply security and hardening best practices
- Add validation capabilities where applicable

Application Sample

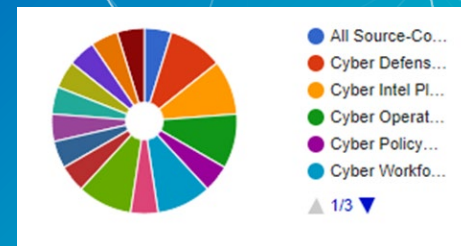
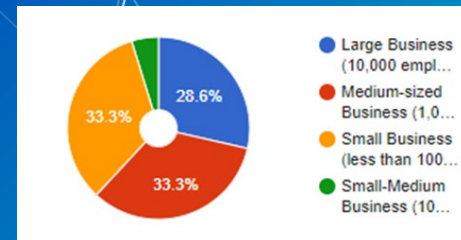
Cyber Supply Chain Risk Survey Tool

- a resource designed for research and education purposes to help organizations manage cybersecurity risks in their supply chain.
- Provides insights into processes and capabilities for addressing cyber supply chain issues
- Questionnaires include contextual data



Implementations to reduce PII exposure

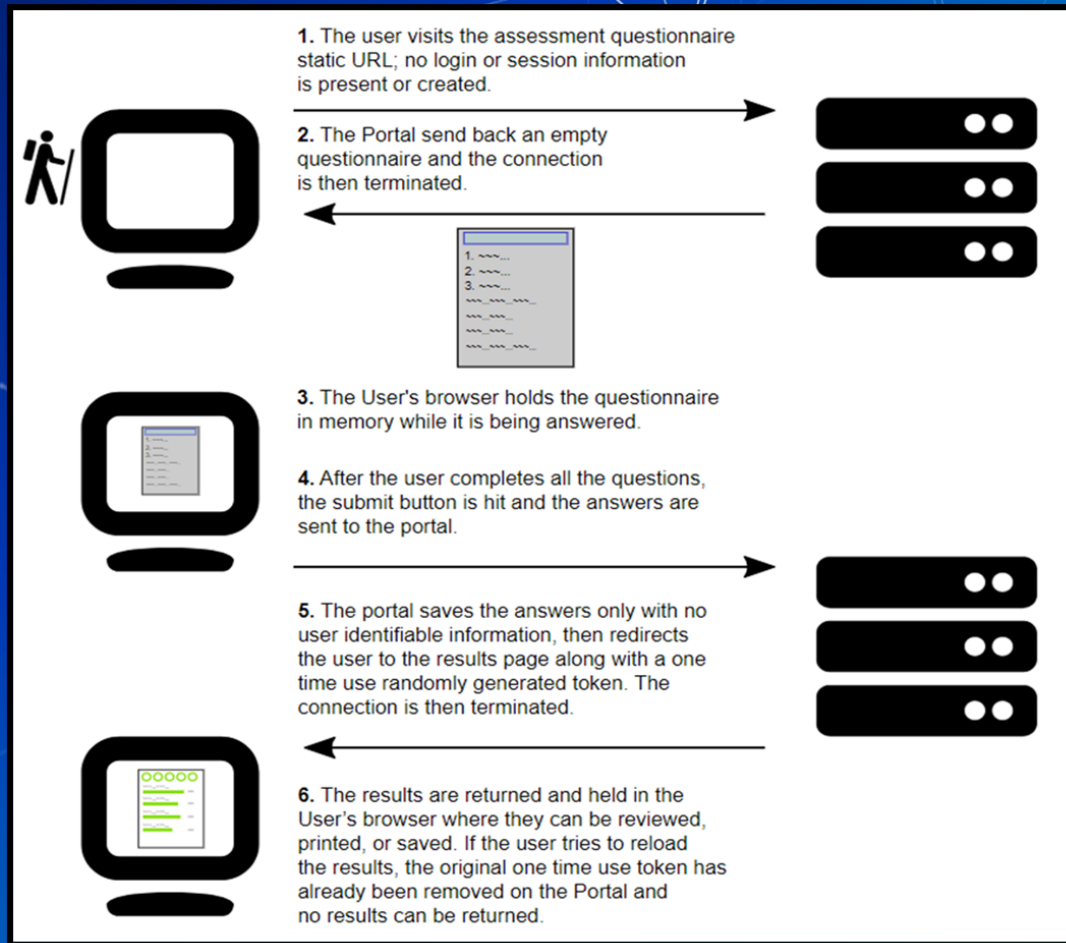
- Remove/modify questionnaires containing PII information
- Anonymize entry
 - no username or password
 - minimize traceback
- Secure data handling
- Validation capability to check for PII



Secure Data Handling

Interactions of an anonymous user with the system

- Separation of the user interface from the server
- Encryption in transit and at rest
- no IP address information is tied to submissions



CRA Contacts

For additional feedback or questions, please contact

- CRA team cyberriskanalytics@nist.gov
- Hung Trinh hung.trinh@nist.gov
- Kate Schroeder kate.Schroeder@nist.gov