Registry Cybersecurity & Privacy

John Pinard
Chief Information Officer, RPRA

December 2019

RPRA Resource Productivity
& Recovery Authority

The Registry

- The Registry is the online database the Authority uses to register producers of materials designated under the *Resource Recovery and Circular Economy Act, 2016* (RRCEA) and other parties obligated by regulations under the RRCEA, and receive information from these parties as required by regulations.
- The Registry is based on the Salesforce platform – a secure cloud-based system that allows the Authority to manage interactions with parties required to register with the Authority and report.
- A custom portal is developed for each regulation that allows registrants under that regulation to report the data required by the regulation.
- Registrants with obligations under more than one regulation only need one account and will be able to meet all of their reporting requirements through that single account.

Protecting Registrants' Data

What data is collected?

- All regulated entities supply corporate business information for registration (e.g., Business Name, Address, Contact Info)
- Producers report sales or supply data
- Producers or their service providers report on performance against collection and management targets

What degree of Security and Privacy is required?

- Sales or supply data submitted by regulated entities is commercially sensitive and highly confidential.
- Security and privacy are critical factors in the design, build, and operation of the Registry.

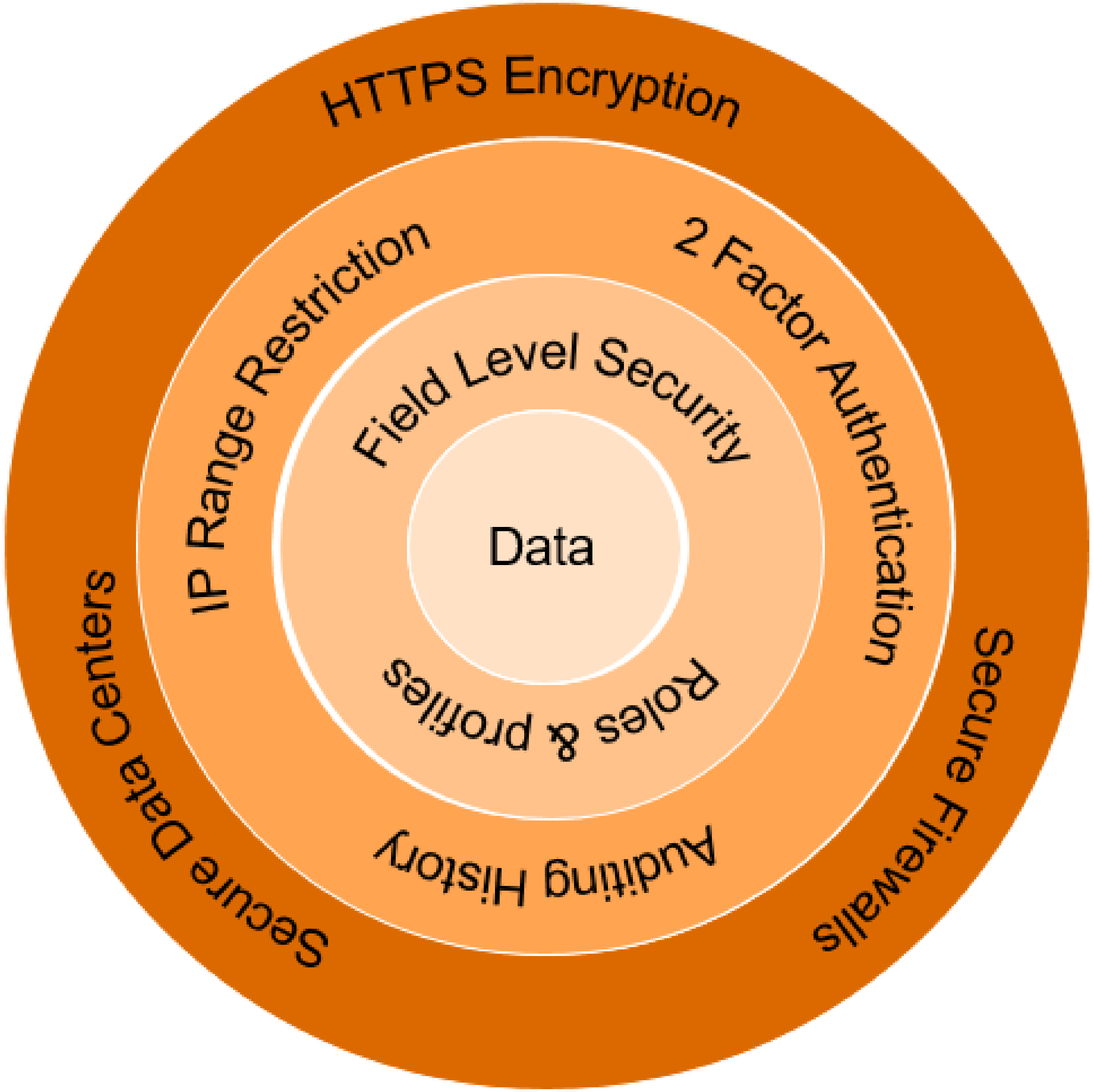
Cybersecurity and Privacy Considerations

Given the highly confidential nature of some of the data submitted via the Registry, cybersecurity and privacy considerations are embedded throughout each Registry project, including:

- Technology Platform - the software platform and architecture selected
- Registry Design - implementation of features that promote cybersecurity and privacy by design
- RPRA Operational Processes - organizational policies, procedures and controls that reinforce strong cybersecurity and privacy practices

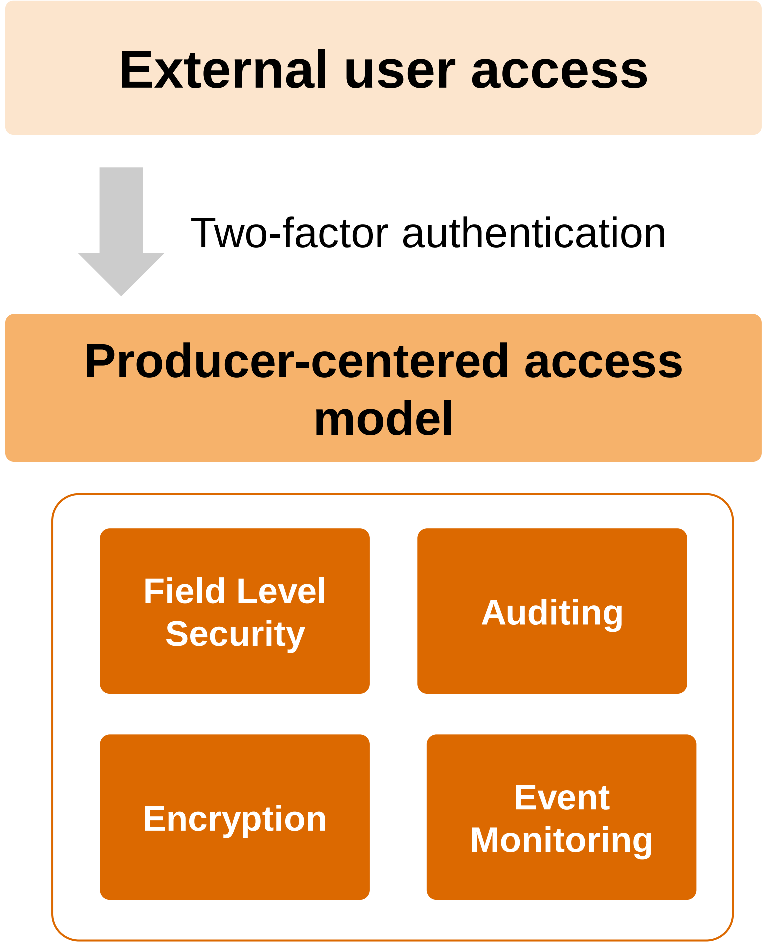
Multiple Lines of Defense

There are several safeguards in place in order to support the security of all data that resides in the Registry.



Registry Design Considerations for Cybersecurity and Privacy

- The Registry can be accessed by two groups of users – external and internal
- **External**: Producers, Producer Responsibility Organizations (PROs) and other service providers
- External users are authenticated using two-factor authentication
- Producer-centric data access and permission model allows Producers to control PRO access to their data
- Auditing for field history and Event Monitoring for key events (e.g., login)



External user access

Two-factor authentication

Producer-centered access model

Field Level Security

Auditing

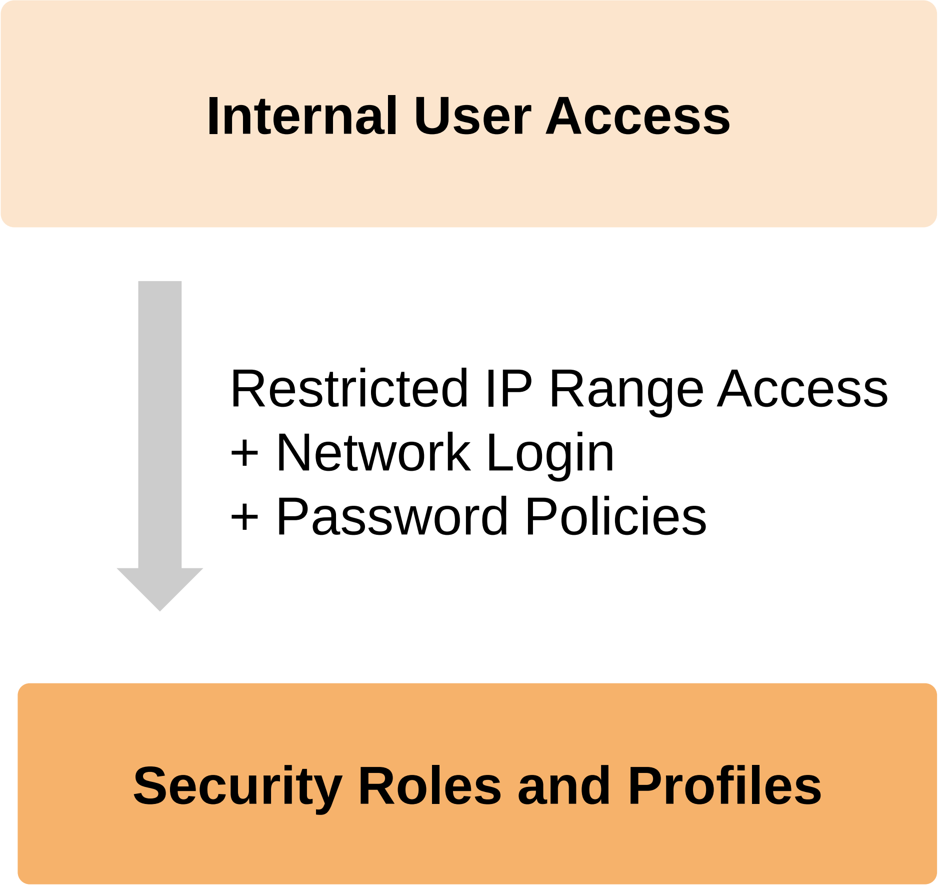
Encryption

Event Monitoring

RPRA Resource Productivity & Recovery Authority

Registry Design Considerations for Cybersecurity and Privacy

- **Internal**: RPRA Staff (e.g., Registry Officers)
- Internal users have role-based access to the Registry from a restricted set of IP addresses
- Auditing for field history and Event Monitoring for key events



Internal User Access

Restricted IP Range Access
+ Network Login
+ Password Policies

Security Roles and Profiles

Resource Productivity & Recovery Authority

Operational Processes - Examples

- Tiers of environmental security to identify the users and their access:
    - Access to physical location
    - Network access
    - Registry System access
    - Role-based data access

- Control around the external primary user and secondary users (limited access/abilities)
    - Modifications to Primary User needs to be done via a business process that involves a Registry Officer (i.e., not a self-serve model)
    - Modifications to Secondary Users can be done only by Primary Users and Registry Officers

- Application of strong privacy by design principles by only capturing the critical data elements required by the regulation

Additional Considerations

- Government of Ontario Information Technology Standards informed the development of the Authority’s cybersecurity policy
- Industry experts engaged to assist in the development of the cybersecurity policy and related procedures
- Authority’s approach to cybersecurity reviewed by the Ministry’s Chief Information Officer and staff to ensure alignment with Ministry standards
- Ongoing review of policies an procedures and system testing