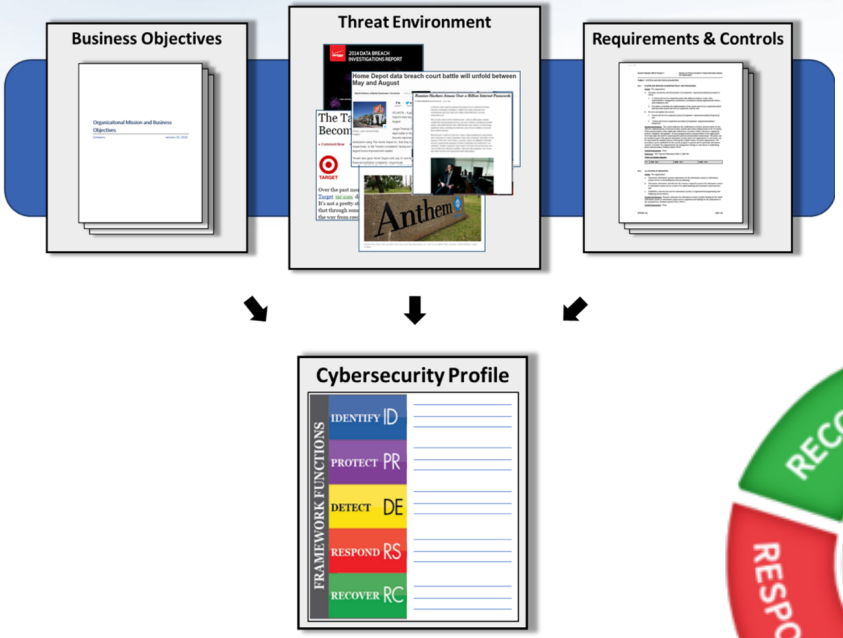
Cybersecurity Framework Election Profiles

Gema Howell, NIST
Gema@nist.gov

Agenda

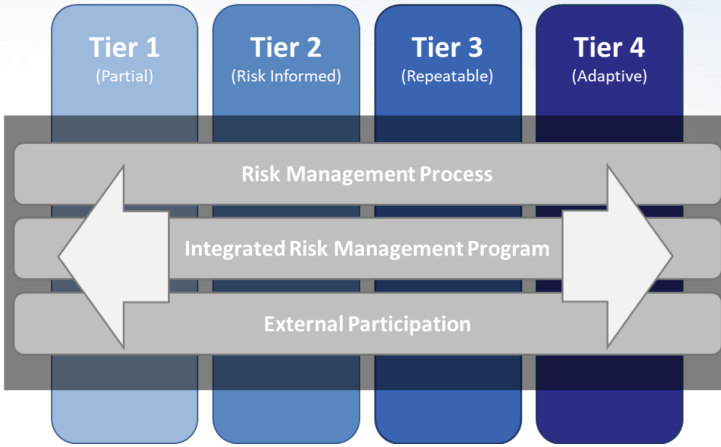
- Give a Brief Cybersecurity Framework Profile Overview
- Recap the Election Infrastructure Profile Work
- Preview the Next Voter Registration Profile
- Share Next Steps

Cybersecurity Framework Components



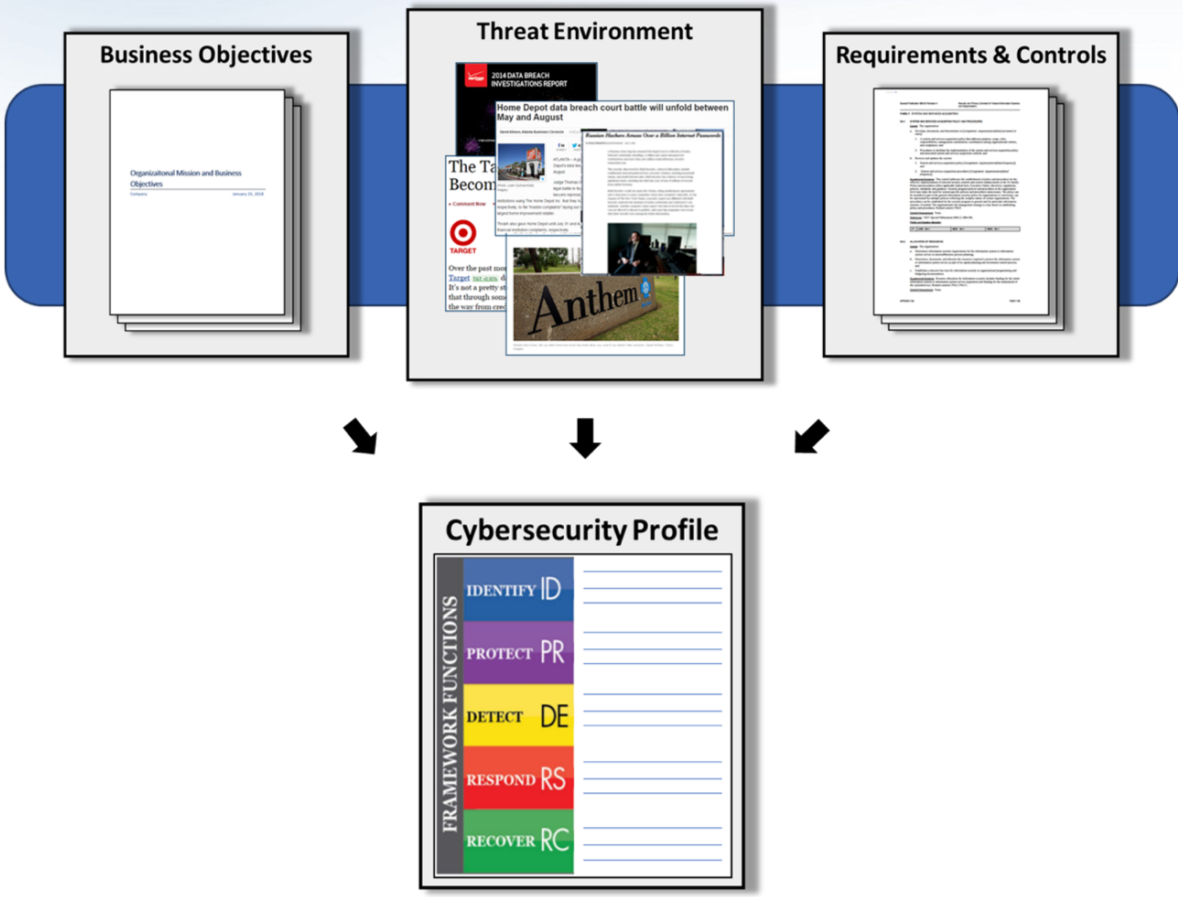
Profile

CORE



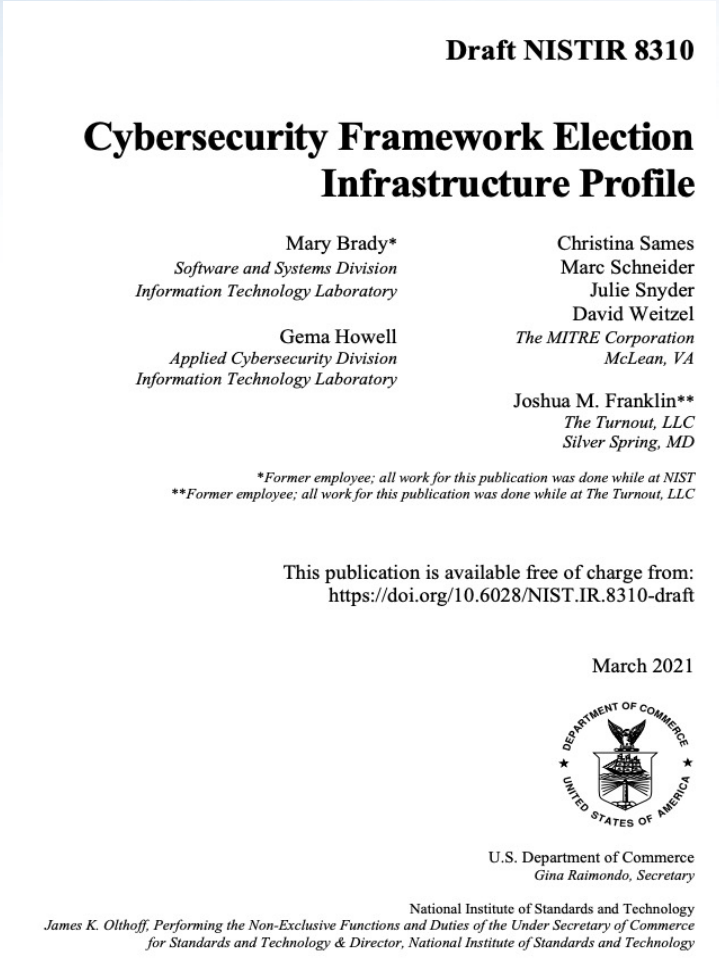
Implementation Tiers

Cybersecurity Framework Profile Overview



- Identifies an organization's business objectives or "**mission objectives**"
- Represents the **desired and prioritized outcomes** based on the mission objectives
- Aligns relevant **standards, guidelines, and practices** address the outcomes
- Can identify opportunities for **improving** an organization's **cybersecurity posture**
- Allows for **self-assessment**
- **Communication** across all parties; Within or outside of an organization

Election Infrastructure (EI) Profile



Draft NISTIR 8310

Cybersecurity Framework Election Infrastructure Profile

Mary Brady*
Software and Systems Division
Information Technology Laboratory

Christina Sames
Marc Schneider
Julie Snyder
David Weitzel
The MITRE Corporation
McLean, VA

Gema Howell
Applied Cybersecurity Division
Information Technology Laboratory

Joshua M. Franklin**
The Turnout, LLC
Silver Spring, MD

*Former employee; all work for this publication was done while at NIST
**Former employee; all work for this publication was done while at The Turnout, LLC

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8310-draft

March 2021

U.S. Department of Commerce
Gina Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Draft NIST Interagency Report (IR) 8310 -

Cybersecurity Framework Election Infrastructure Profile

Document Status

- Public comment closed May 14th
- Gathered and reviewed comments.

- Thank you to all who provided feedback.

EI Profile Overview

What you'll find in the document:

- Info about how we engaged with election stakeholders for input through workshops
  - This included participants from the Election Infrastructure Subsector Government Coordinating Council (GCC) and the Sector Coordinating Council (SCC)
- Prioritized Mission objectives
- Prioritized Categories for each Mission objective – Programmatic Outcomes (e.g., Asset Management)
- Prioritized subcategories for each mission objective - specific outcomes of technical and/or management activities (e.g., Data-at-rest is protected).

EI Profile Mission Objectives

Priority	*Mission Objective*
1	Conduct and Oversee Voting Period Activities†
2	Prepare and Maintain Election Systems†
3	Process and Maintain Voter Registration†
4	Prepare for a Specific Election†
5	Perform On-Going Election Administration Functions
6	Conduct Audits
7	Conduct Election "Wrap-Up" Activities
8	Manage Crisis/Strategic Communications
9	Oversee Office Administration
10	Maintain Workforce

† Identifies the highest priority, or top, mission objectives.

Example Mission Objective Description

3. **Process and Maintain Voter Registration**†. This mission objective encompasses all aspects of data and systems associated with voter registration, specifically, processing voter registration data/information, ensuring the privacy and security of voter information, and maintaining the systems associated with those processes. This mission objective represents *an ongoing process* including election day registration, where allowed. The following is a list of some activities relevant to this mission objective:
    - Maintain voter registration list/database
    - Maintain voter registration website
    - Process voter registrations
    - Release information to 3rd parties as allowed or required by law

    Rationale: This mission objective represents critical precursor activities vital to ensuring qualified citizens can properly vote and maintaining the integrity and security of voter information, upon which hinges the confidence of the electorate in an election outcome.

Category Prioritization

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Ranking Options:

- **High Priority (H)** Categories were considered the most critical for accomplishing a Mission Objective.
- **Moderate-Possibly-High Priority (M-H)** Categories were considered important to Mission Objective, although not as important as High Priority Categories.
- **Moderate Priority (M)** Categories were prioritized for a Mission Objective, but not with the same urgency as other priority Categories.

Example Category Prioritization

Table 5 - Process and Maintain Voter Registration (MO #3)

CSF Function	High Priority	Moderate-Possibly High Priority	Moderate Priority
IDENTIFY	N/A	N/A	N/A
PROTECT	Access Control (PR.AC) Data Security (PR.DS)	N/A	N/A
DETECT	N/A	Anomalies and Events (DE.AE)	N/A
RESPOND	N/A	N/A	Response Planning (RS.RP)
RECOVER	N/A	N/A	Recovery Planning (RC.RP)

Subcategory Prioritization

Function	Category	Subcategory
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices users, and processes
		PR.AC-2: Physical access to assets is managed and protected
		PR.AC-3: Remote access is managed
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and

Ranking Options:

- **High Priority (●●●):** The most critical Subcategories for enabling a Mission Objective and should be addressed immediately given available resources.
- **Moderate Priority (●●):** Subcategories that could be as urgent as High Priority Subcategories but most likely only in certain contexts or environments. They may not need not be addressed as immediately as High Priority Subcategories.
- **Other Priority (●):** Subcategories that are important to the overall cybersecurity of the Mission Objective but may not require the same level of urgency as higher priority Subcategories.

Example Subcategory Prioritization

Table 26 - Anomalies and Events (DE.AE) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	•	•	•	••	•••	•	•	•	•	•••	•
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	•	•	•	•••	•••	•	••	•••	•	•	•
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	•	•	•	•	•	•	•••	••	•	••	•
		DE.AE-4: Impact of events is determined	•	•	•	•••	•	•	•••	••	•••	••	•
		DE.AE-5: Incident alert thresholds are established	•	•	•	•••	•	•	•••	••	••	•••	•

Recap

- NIST IR 8310 *Cybersecurity Framework Election Infrastructure Profile* draft is available
- The document gives a walk through of the steps to develop the Election Infrastructure profile
- This profile can be used as an example election profile or a baseline profile.

Potential Uses or Benefits

- Repeatable process to improve cybersecurity posture
- Stronger communication throughout an organization using a common language
- Flexible activities that can be tailored to your needs
- Identify any gaps or opportunities for improvement

Related Work

Election Infrastructure Profile Usability Research

- NIST worked with the Center for Tech and Civic Life to hold workshops to look into the usability of the cybersecurity framework profiles
- This included stepping through the profile development process
- Gathered information and feedback
- Provided recommendations for improving the usability of the profiles

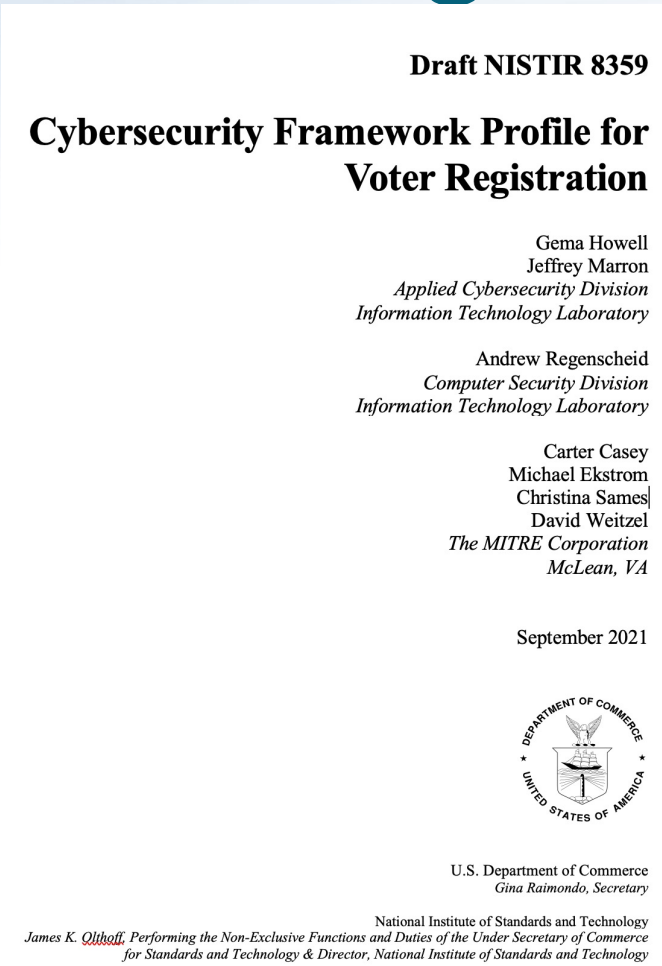
Related Work (cont.)

RECOMMENDATION

In any accompanying materials or presentations, stress that both large and small election departments have been targets of cyber attacks. Show brief case studies or news headlines to demonstrate the risk to small local election offices.

"I've been a part of a bunch of different cybersecurity initiatives. [. . .] And they're very technical. So, I appreciate that this is sort of a general overview with developing a plan on how to prioritize, as opposed to already assuming that you've got specific knowledge of what you want to do" – ***Anonymous Application Administrator, Anonymous New England municipality #2***

Voter Registration (VR) Profile



Draft NISTIR 8359

Cybersecurity Framework Profile for Voter Registration

Gema Howell
Jeffrey Marron
Applied Cybersecurity Division
Information Technology Laboratory

Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

Carter Casey
Michael Ekstrom
Christina Sames
David Weitzel
The MITRE Corporation
McLean, VA

September 2021

U.S. Department of Commerce
Gina Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

Document Status

- Not publicly available yet
- Need to get additional feedback from election stakeholders

Next Steps

- Coordinate next steps for VR profile with the DHS Cybersecurity Framework Joint Working Group
- Update both documents based on public comment and publish
- Incorporate results from the usability research
- Consider providing additional informative references – standards, guidelines, and best practices that align with the outcomes

Questions?

Gema Howell, NIST
Gema@nist.gov