The NIST Cybersecurity Framework: What it means for elections

Mike Garcia
Senior Advisor for Elections Best Practices
mike.garcia@cisecurity.org
What is the NIST CSF?

**NIST CSF**: prioritized, flexible, and cost-effective framework to manage cybersecurity-related risk. Helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.
NIST CSF: framework

– puts the organize in your organization
What really matters

Drives a standardized approach to security

– Standard here means repeatability and comparability; it turns amorphous cybersecurity blah blah into apples

Works for all orgs regardless of size or substance

– The content is applicable to all; it’s up to the org to place the goalpost
The good and bad

**Pros**
- (Mostly) understandable by non-technical readers
- Can be completed quickly or in great detail to suit the orgs needs
- Has a ‘self-contained’ maturity model—helps you understand what’s right for your org and track to it
- Highly flexible for different types of orgs

**Cons**
- Better suited for diagnostic, organizational, and planning than for executing
- Helps you focus; doesn’t tell you what to do or how to do it
Truly a framework

Gives orgs “a common taxonomy and mechanism to:

1. Describe their current cybersecurity posture;
2. Describe their target state for cybersecurity;
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4. Assess progress toward the target state;
5. Communicate among internal and external stakeholders about cybersecurity risk.”

5 functions, 23 categories, and 108 subcategories identify, protect, detect, respond, recover

Has implementation tiers for maturity and profiles to customize
Example:

- Function: **Protect (PR)**
- Category: **Identity Management, Authentication and Access Control (PR.AC)**: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
- Subcat: **PR.AC-1**: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
NIST CSF Election Profile

• CSF profiles (in general)
  – Takes business objectives, the threat environment, and specific reqs and controls into consideration

• Election profile
  – Prioritizes (high, mod-to-high, mod) among the 108 sub-cats
  – Example: 12 high, 28 mod-to-high, 14 mod
A widely accepted tool
  – Best as an executive diagnostic and communication tool
  – Structured for setting organizational targets and objectives

Helps organize a complex system

Coupled with profile, yields a framework by which to organize effort and a prioritization by which to attack it
Thank You