ALASKA NATIVE
**TRIBAL HEALTH**
CONSORTIUM

## OUR VISION:

Alaska Native people are the healthiest people in the world.

# NIST Cybersecurity Framework Assessment and Compliance

ANTHC IT Security

# What is the NIST Cybersecurity Framework?

- Framework for managing cybersecurity risk
- Published by United States National Institute of Standards (NIST)
- Current version is 1.1 published in 2018
- CSF Version 2.0 is under development

# Benefits of Using NIST CSF

- Uses industry recognized benchmarks to reduce cybersecurity risk
- Can use as foundational document for cybersecurity program
- Provides metrics for measuring risk and tracking program maturity
- Prioritize investments to maximize impact
- Demonstrates commitment to cybersecurity
- Allows for industry peer comparison

# Establishes a Common Taxonomy

- Describe their current cybersecurity posture
- Describe their target state for cybersecurity
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- Assess progress toward the target state
- Communicate among internal and external stakeholders about cybersecurity risk

# NIST CSF Components

- Framework Core
- Framework Implementation Tiers
- Framework Profile

# Framework Core

- Functions
  - Used to organize cybersecurity activities
  - Align with incident response methodologies
- Categories
  - Groups of cybersecurity outcomes
- Subcategories
  - Specific outcomes (controls)
- Informative Resources
  - Resources to assist in achieving outcomes

# NIST CSF Functions

- Identify (ID)
  - Identify and manage cybersecurity risk
- Protect (PR)
  - Develop and implement safeguards
- Detect (DE)
  - Identify the occurrence of a cybersecurity event
- Respond (RS)
  - Actions to take during incident
- Recover (RC)
  - Restore services  (cyber resilience)

# NIST CSF Functions and Categories

| Function ID | Function | Category ID | 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 | Identity Management, Authentication and 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 |

# NIST CSF Subcategories

- Subcategories are the controls measured to determine NIST CSF compliance
- Identify specific actions to achieve category outcome
- Subcategories are used to measure program maturity
- CSF has 108 subcategories
- Nomenclature makes them easy to identify

# CSF Informative Resources

- References to established standards, guidelines, and practices that can be used to achieve subcategory outcomes
- Examples include:
  - CIS Critical Controls
  - NIST SP 800-53 Rev. 5
  - ISO/IEC 27001:2013
  - COBIT 5
  - Others

# CSF Implementation Tiers

- Describe risk management practices
- Organizations should determine desired Tier
- Four Tiers
  - Partial
  - Risk Informed
  - Repeatable
  - Adaptive
- Tiers are not maturity levels

# Framework Profile

- Identify current state or target state of specific cybersecurity activities
- Illustrate alignment of subcategories and business objectives
- Align subcategories with specific threat to determine security posture
- Roadmap for desired cybersecurity alignment with CSF
- Profile examples can be found on NIST site

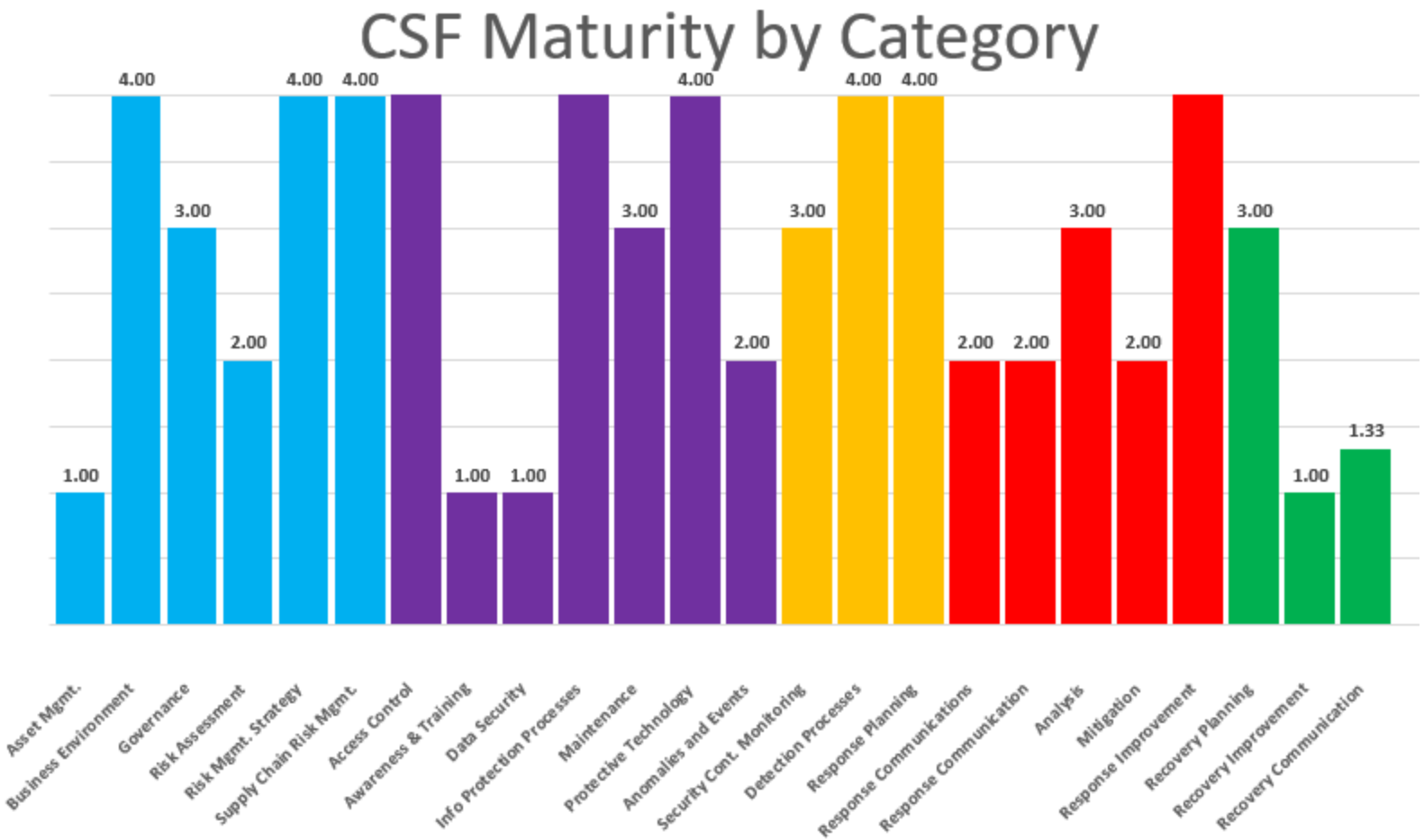
# CSF Assessment

- Download Excel version of CSF
- Prepare spreadsheet
  - Clear formatting, table format
- Determine scoring system
  - Consider qualitative method to start
  - Migrate to quantitative method later
- Add date column and enter score for each subcategory

# CSF Assessment, cont.

- Download spreadsheet
- Clear all formats and fill in missing values
- Add column for label name on chart
- Add column for date
- Add score for each subcategory
- Name data table
- Subtotal data based on score(s)
- Use a pivot chart to display data

# Example Maturity Chart



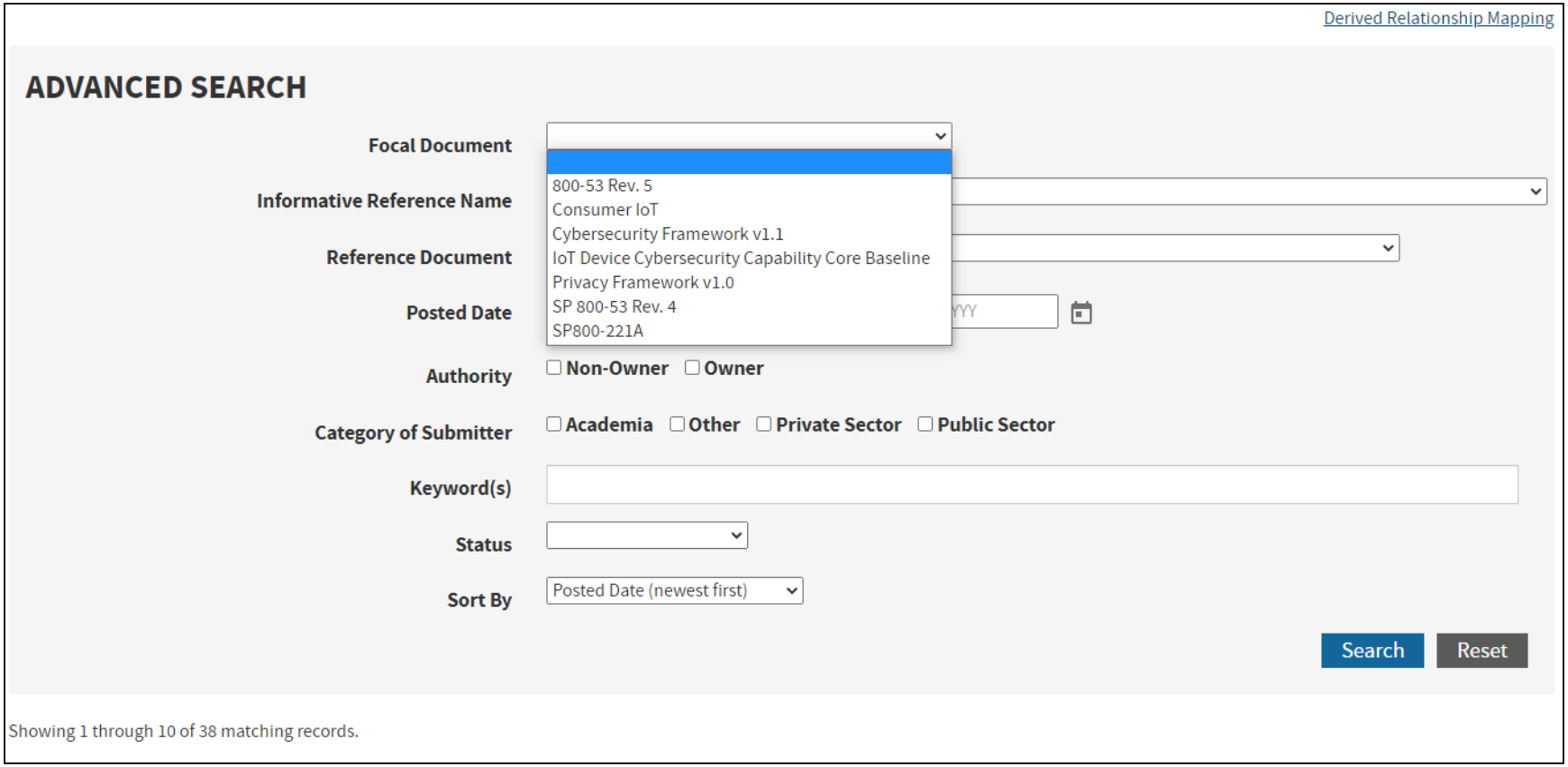
# Other Ways to Report on CSF Compliance

- Roll-up data to show CSF function maturity
- Use to create profiles and compare current and target states
- Compare program progress over time
- Use process to evaluate current state for other frameworks
- The possibilities are endless

# NIST OLIR

- National Online Informative References Program
  - https://csrc.nist.gov/projects/olir
- Informative Reference Catalog
  - https://csrc.nist.gov/Projects/olir/informative-reference-catalog
- Provides a crosswalk for different documents

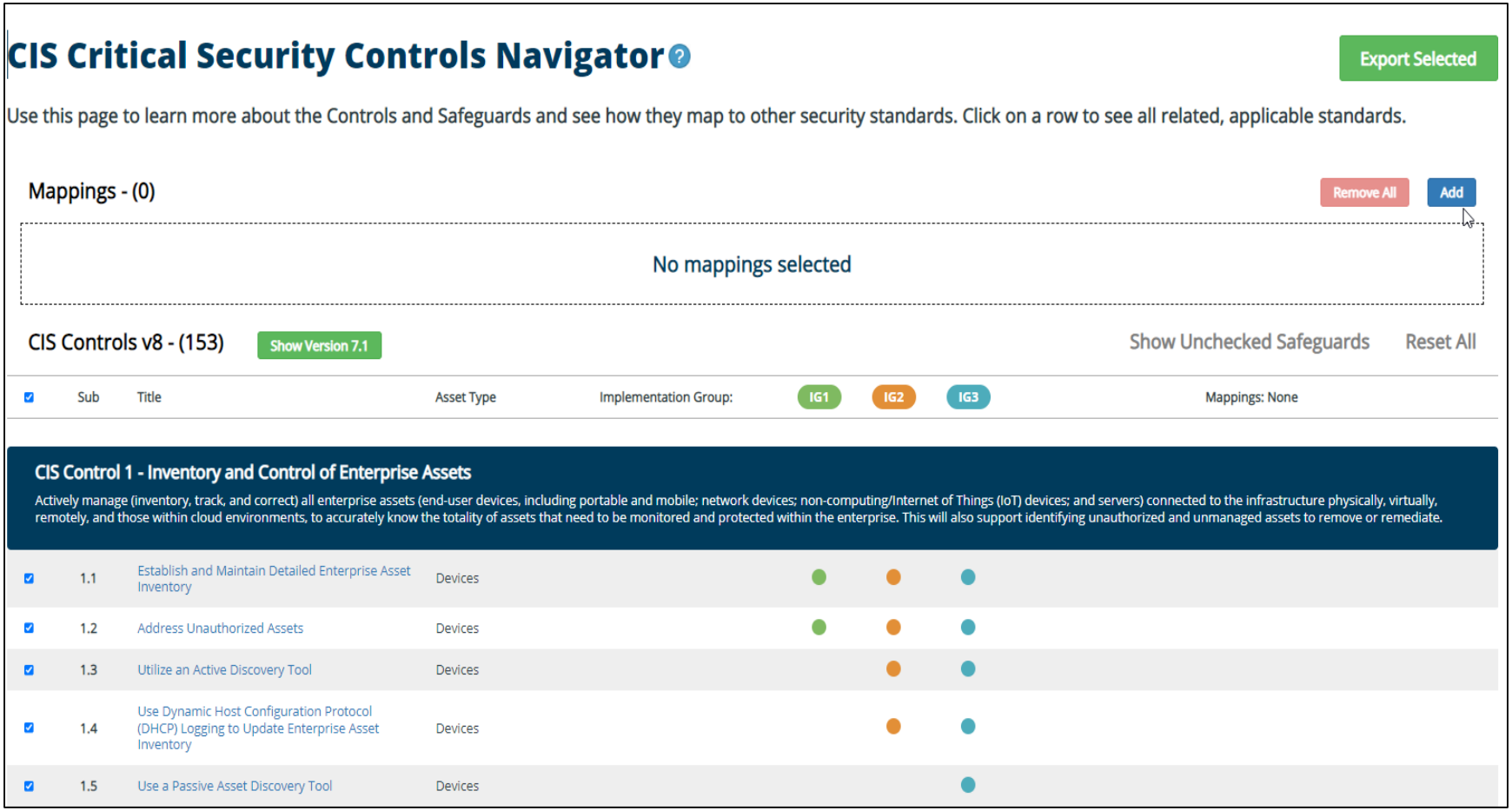
# NIST OLIR, cont.



# CSF to CIS Controls Mapping

- Provides spreadsheet mapping CSF to CIS Controls
- CIS Navigator
  - https://www.cisecurity.org/controls/cis-controls-navigator/

# CSF to CIS Controls Mapping, cont.



## CIS Critical Security Controls Navigator

Export Selected

Use this page to learn more about the Controls and Safeguards and see how they map to other security standards. Click on a row to see all related, applicable standards.

Mappings - (0)

Remove All | Add

No mappings selected

CIS Controls v8 - (153) Show Version 7.1

Show Unchecked Safeguards | Reset All

| Sub | Title | Asset Type | Implementation Group: | IG1 | IG2 | IG3 | Mappings: None |
|---|---|---|---|---|---|---|---|
| **CIS Control 1 - Inventory and Control of Enterprise Assets** Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate. | | | | | | | |
| 1.1 | Establish and Maintain Detailed Enterprise Asset Inventory | Devices | | ● | ● | ● | |
| 1.2 | Address Unauthorized Assets | Devices | | ● | ● | ● | |
| 1.3 | Utilize an Active Discovery Tool | Devices | | | ● | ● | |
| 1.4 | Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory | Devices | | | ● | ● | |
| 1.5 | Use a Passive Asset Discovery Tool | Devices | | | | ● | |

# CSF to CIS Controls Mapping, cont.

- [ ] Azure Security Benchmark v3
- [ ] CISA Cybersecurity Performance Goals
- [ ] CMMC v2.0
- [ ] Criminal Justice Information Services (CJIS) Security Policy
- [ ] CSA Cloud Controls Matrix v4
- [ ] Cyber Essentials v2.2
- [ ] Cyber Risk Institute (CRI) Profile v1.2
- [ ] Federal Financial Institutions Examination Council (FFIEC-CAT)
- [ ] GSMA FS.31 Baseline Security Controls v2.0
- [ ] HIPAA
- [ ] ISACA COBIT 19
- [ ] ISO and IEC 27002:2022 Information Security Controls
- [ ] MITRE Enterprise ATT&CK v8.2
- [ ] New Zealand Information Security Manual v3.5
- [ ] NIST CSF
- [ ] NIST SP 800-171
- [ ] NIST SP 800-53 Revision 5 Low Baseline
- [ ] NIST SP 800-53 Revision 5 Moderate Baseline
- [ ] North American Electric Reliability Corporation-Critical Infrastructure Protection Standards (NERC-CIP Standards)
- [ ] NYDFS Part 500
- [ ] PCI v3.2.1
- [ ] PCI v4.0
- [ ] SOC 2

# Contact Information

Lorri Booher - ANTHC IT Security
lmbooher@anthc.org
907-317-3147


gunalchéesh • qagaasakung • igamsiqanaghhalek • ‘awa’ahdah • tsin’aen • baasee’ • quyanaa • dogidinh • way dankoo • háw’aa • mahsi’ • maasee’ • chin’an • quyana • quyanaq • quyanaa

ALASKA NATIVE
**TRIBAL HEALTH**
CONSORTIUM