National Cybersecurity Center of Excellence (NCCoE)

Electric Vehicle/eXtreme Fast Charging Infrastructure
Cybersecurity Framework Profile Introductory Meeting

February 16, 2023

This webinar is being recorded

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

Submitting Questions

Please use the Q&A window to enter your questions.

1. To open the Q&A panel, click on the ellipses at the bottom of the screen for 'More Panels' and click on Q&A.

2. Type your question in the text box and click Send

Agenda

Time	Session Title	Speaker(s)
2:00-2:03	Webinar Kick-off	
2:03-2:05	Welcome to the NIST / NCCOE	• Jim McCarthy, Senior Security Engineer, NIST NCCoE
2:05-2:15	Opening Remarks	• Fowad Muneer, Department of Energy
2:15-2:25	Overview of NCCoE EV XFC Cybersecurity Framework Profile	• NCCoE Project Team
2:26-3:15 Electric Vehicle/eXtreme Fast Charging Infrastructure Cybersecurity Framework Profile Introductory Meeting	EV XFC Panel discussion	Moderator: Pete Tseronis, Dots and Bridges • Sean Plankey, Bedrock • Teza Mukkavilli, Charge Point • Lee Slezak, Department of Energy • Sunil Chhaya, Electric Power Research Institute
3:15-3:28	Live Q&A	
3:28	Closing Remarks	• James McCarthy, Senior Security Engineer, NIST NCCoE

Welcome to the NIST / NCCOE

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

A NIST Applied Cybersecurity Center

Jim McCarthy
Senior Security Engineer,
National Cybersecurity Center of Excellence,
National Institute of Standards and Technology

Who We Are

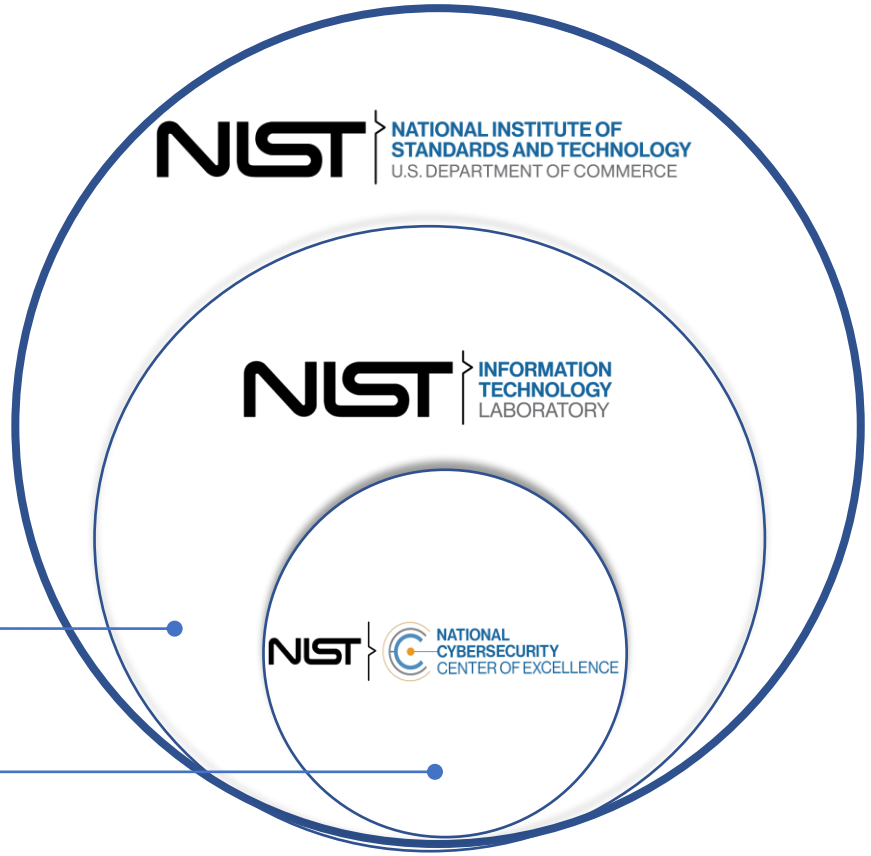
NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

An **open, transparent** and **collaborative** hub addressing complex cybersecurity problems

Who We Are

Part of NIST, the NCCoE has access to a foundation of expertise, resources, relationships, and experience.

NIST is a **non-regulatory** agency. Adoption and use of our guidance is **voluntary**.



Opening Remarks

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Fowad Muneer
Acting Deputy Director, Risk Management Tools and Technologies,
Office of Cybersecurity, Energy Security, and Emergency Response,
Department of Energy

NCCoE Team Introduction

Jim McCarthy

NIST

Nakia Grayson

NIST

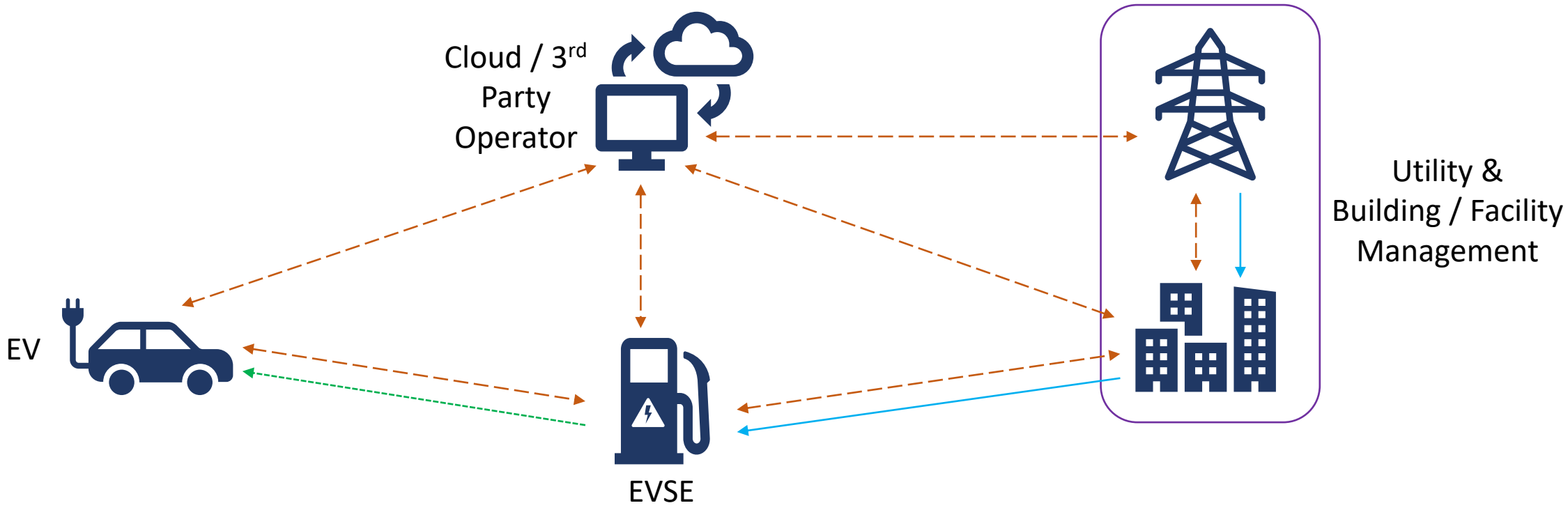
Josie Long

MITRE

Michael Thompson

MITRE

EV XFC Ecosystem Scope



Four Components of the EV Charging Ecosystem

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

EV Supply Equipment (EVSE)

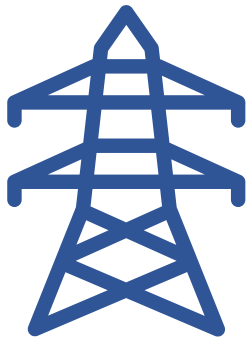
- EV charging stations
- Networked connectivity with EV and cloud
- Built-in charging management and data processing capabilities
- Thermal management systems for charging equipment

Electric Vehicle (EV)

- Internal Control Area Network between various vehicle systems
- Networked connectivity with EVSE and cloud
- Built-in charging management
- Smartphone application connectivity

Cloud/3rd Party (Charging Networks)

- Business logic and user account management
- Operations management
- Payment processing interfaces
- EV/EVSE data aggregation management
- Data security functions



Utility & Building Management

- EVSE power supply
- Building/facility management for linked EVSE installations
- Grid services such as peak shaving, demand response, usage statistics, load shifting, etc.

Cybersecurity Risks

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Resiliency

- Unsecure communication to utilities can disrupt power flow causing reliability issues
- Jamming the charging station by creating severe interference can make it unusable
- Modifying firmware limits ability to charge, over charge, or discharge a battery at attacker's will

Safety

- Charging stations are subject to physical tampering, especially in remote locations
- Gaining electronic access to charging stations can disable battery pack safety systems
- Modifying firmware can communicate wrong charging parameters posing a safety risk

Financial

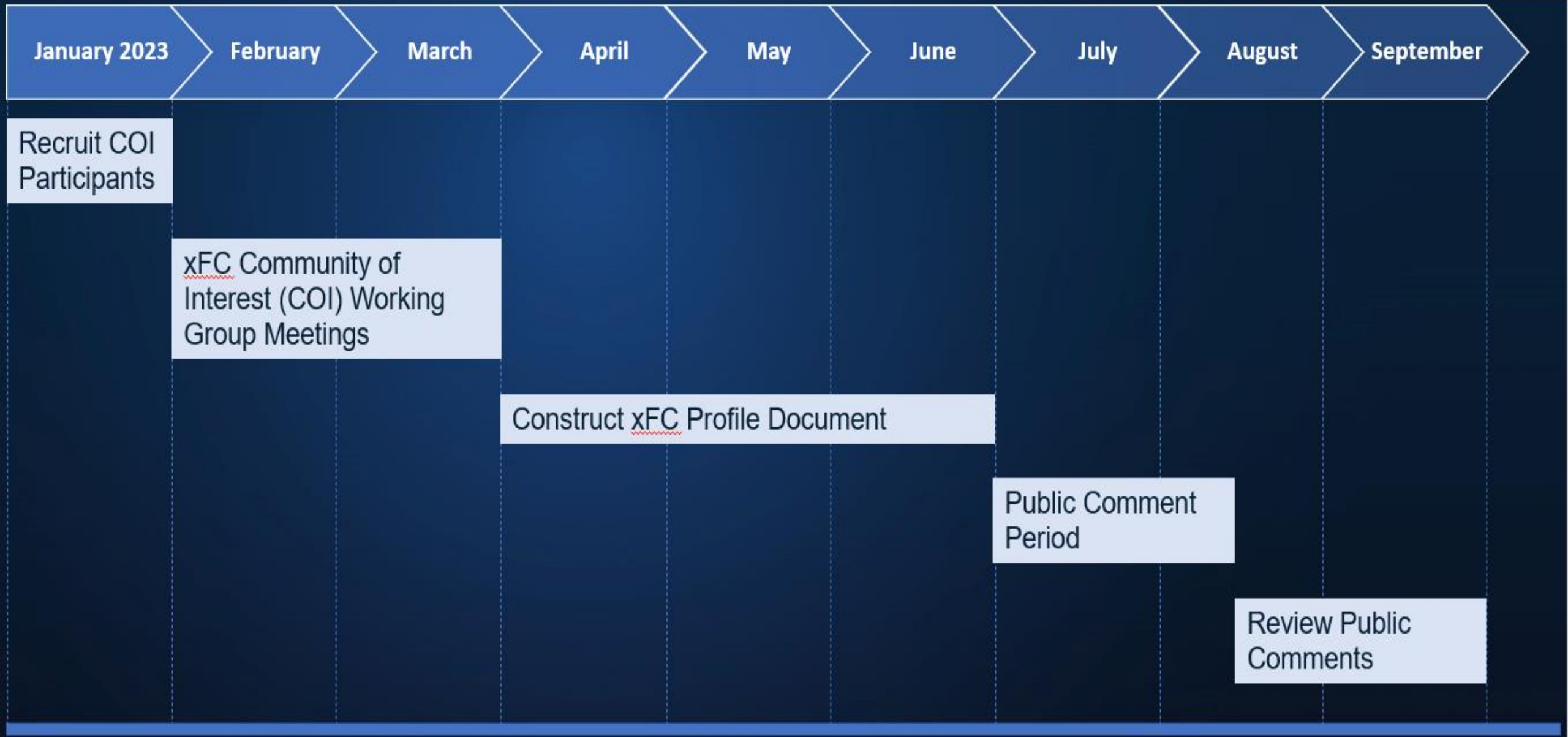
- Gaining root access to cloud can release all customer data
- Skimmer applied to charging station collects payment information
- Unencrypted wireless communications may allow release of financial data

Privacy

- Trusted insiders may gain access to sensitive information, including PII
- Authentication details intercepted from wireless transmissions allows attacker to impersonate user
- Spy chip attached to EV revealing usage patterns

EV XFC CSF Profile Timeline

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Cybersecurity Framework (CSF) Overview

NIST Cybersecurity Framework

- Common and accessible language
- Adaptable to many technologies, lifecycle phases, sectors, and uses
- Risk-based
- Living document
- Guided by many perspectives – private sector, academia, public sector

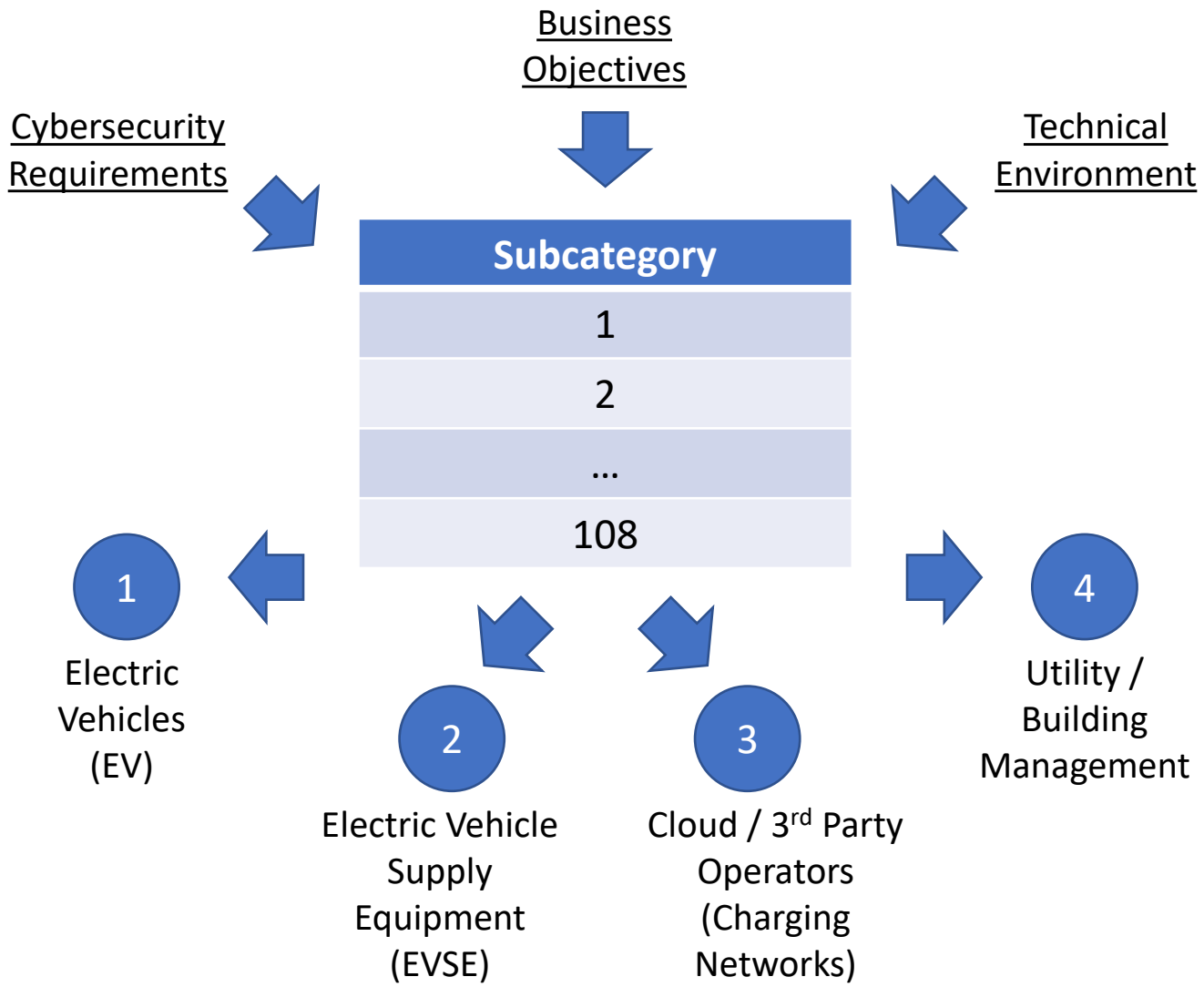
Framework Core Establishes a Common Language

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

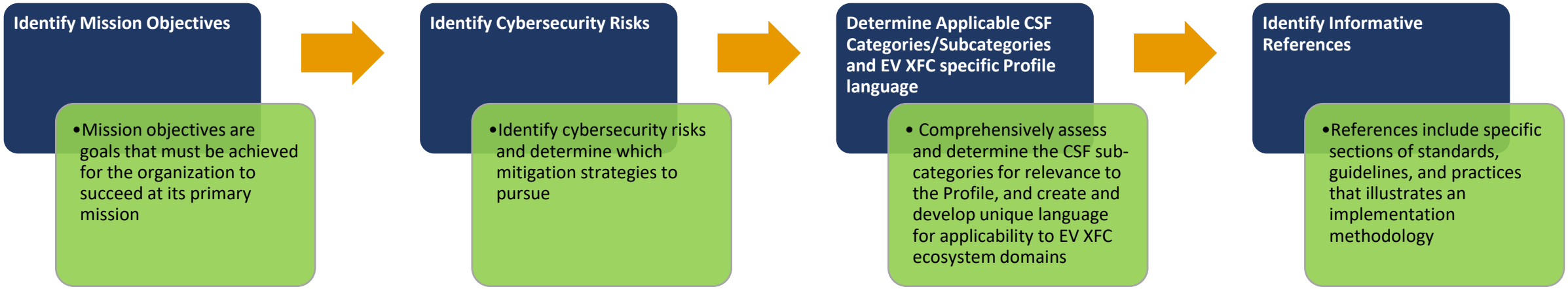
Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Cybersecurity Framework Profiles

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE



Profile Development



Example: PNT Profile

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Function

Category

Subcategory

Subcategory ID

CSF language

Guidance on how to apply the subcategory to organizations that rely on PNT services

PNT specific references on how to implement controls to achieve the desired outcomes of the EO

Identify Asset Management		
Subcategory	**Applicability to PNT**	**References (PNT-Specific)**
AM-1: **Physical devices and systems within the organization are inventoried.**	Document and maintain an inventory of the PNT system components that reflect the current system. The physical inventory should include PNT system components used to support critical infrastructure/operations and critical system components that rely on PNT data and services to properly function. PNT system components may include GNSS receivers, wireless local area network (WLAN) receivers, terrestrial beacon system receivers (TBS), radio navigation or timing antennas, network switches, Internet of Things (IoT)/ Supervisory Control and Data Acquisition (SCADA) devices, NTP and Precision Time Protocol (PTP) servers, positioning sensors, clocks, etc. Cryptographic modules, test and measurement equipment, navigation systems, etc. are examples of hardware and devices dependent on PNT services. Incorporate a configuration management tool that documents locations of all PNT antennas and verify with physical inspections. During physical inspections, identify equipment associated with PNT devices and locate PNT service provider interfaces, such as GNSS antennas.	**3GPP TS 36.305** 4.2 **DHS CISA** 1.a, 2.a **ICAO 9849** 1.4 **IEEE 1588** 6, 9, 10 **IEEE 802.1AS** 7, 11 **IEEE 2030.101** 4.6, 4.7, 4.8, 4.9 **NIST SP 800-53 Rev. 5** CM-8, CM-9 PM-5 **NIST SP 800-160 Rev. 1** 2.3 **RTCA 229** 2.1.5.2.1, 2.4, 2.5 **RTCA 292** 2.5 **RTCA 326** 3.1 **USG FRP** 1.7.8, 4.4.2, 4.6, 5.1.2, 6

Join the EV XFC CSF Profile Community of Interest (COI)

First EV XFC CSF Profile Working Meeting: Thursday 02/23/2023, 2:00 p.m. – 3:30 p.m. EST

Email us at: evxfc-nccoe@nist.gov

Visit our project page:
https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-electric-vehicle-extreme-fast-charging-infrastructure

Link to PNT Profile :
Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services (nist.gov)

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Panel Discussion

EV XFC Panelists

Pete Tseronis (moderator)

Dots and Bridges

Sean Plankey

Bedrock Systems

Teza Mukkavilli

ChargePoint EVSE

Lee Slezak

Department of Energy (DoE)

Sunil Chhaya, Ph.D

Electric Power Research Institute (EPRI)

Submitting Questions

Please use the Q&A window to enter your questions.

1. To open the Q&A panel, click on the ellipses at the bottom of the screen for 'More Panels' and click on Q&A.

2. Type your question in the text box and click Send


NIST
NATIONAL
CYBERSECURITY
CENTER OF EXCELLENCE
nccoe.nist.gov
@NISTcyber