USAID FROM THE AMERICAN PEOPLE | ENERGY POLICY ACTIVITY

CYBERSECURITY DAY

Cybersecurity in the Energy Community Case Study – Bosnia and Herzegovina

June 1, 2021

Energy Community Secretariat

AGENDA

- Introduction USAID EPA Project
- Summary of report
- Specific EU Cyber Security regulation for the Energy Sector
- Specific Cyber Security standards relevant for the Energy Sector
- International good practices from EU member states
- Information Sharing and Analysis Center (ISAC)
- Recommendations

USAID Energy Policy Activity, Bosnia and Herzegovina

USAID Energy Policy Activity project activities

- Helping BiH to coordinate, manage, and improve transparency in the gas and electricity sectors
- Cooperation with the OSCE Mission in BiH (Organization for Security and Co-operation in Europe) – Neretva Cybersecurity Working Group
- Working group and SOW
- Road Map for the implementation of NIS Directive in the BiH energy sector
- Developed documents (Gap analysis and Int'l best practice)

Energy Policy Activity (EPA)

Policy and Technical Assistance Project

Total Funding: $7.5 million

Project Duration: September 2019 - 2024

Implementing Partner:
Advanced Engineering Associates International

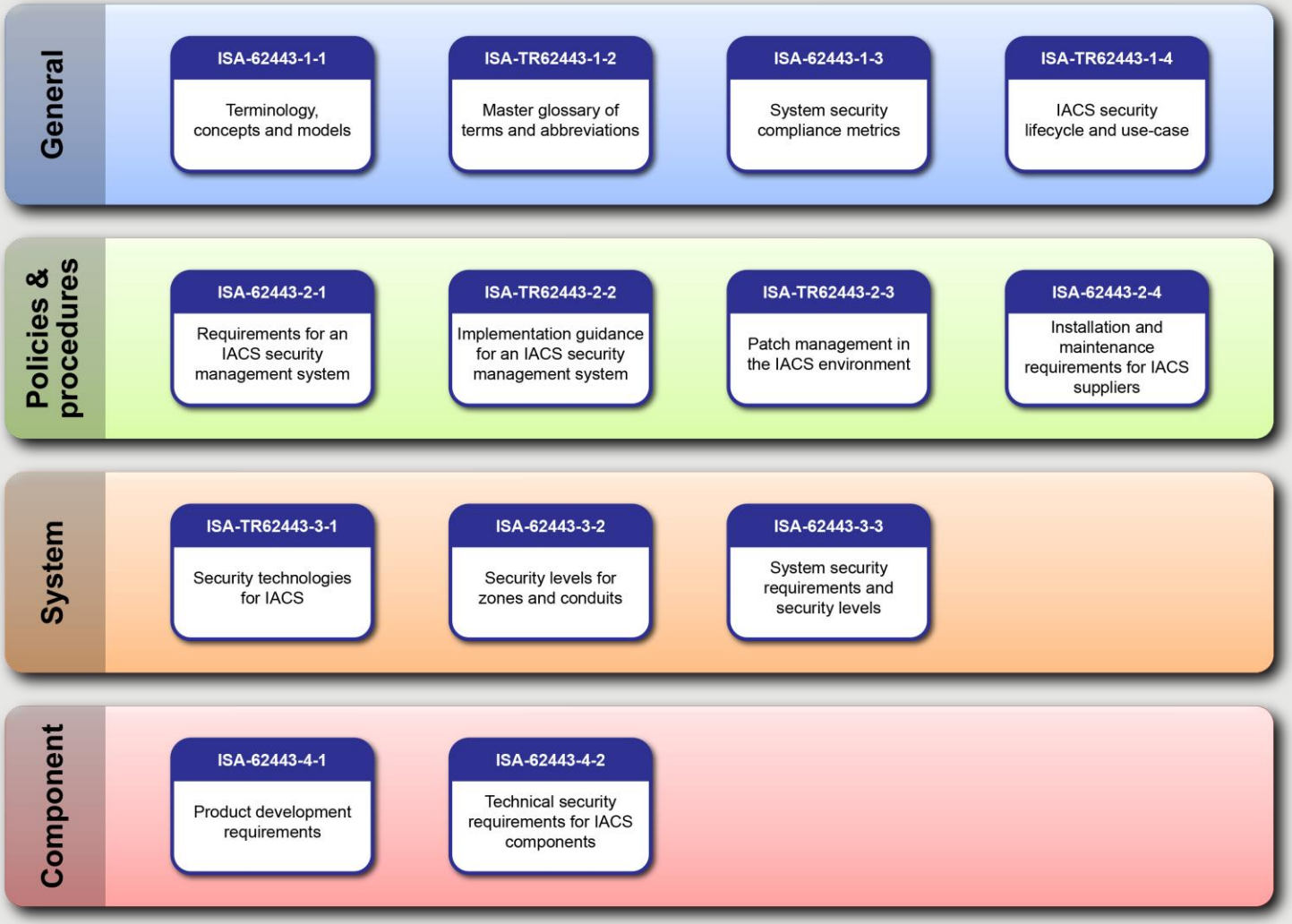
Draft report on International best practices

- EU Cybersecurity legislation/regulation/standards
- Specific EU Cyber Security regulation for the Energy Sector
- Specific Cyber Security standards relevant for the Energy Sector
  - EU
  - US
- International compliancy practices from similar (EU) Member State
  - Portugal
  - Italy
  - Austria
  - The Netherlands
  - Germany
- Information Sharing and Analysis Center (ISAC)
- Recommendations from the author

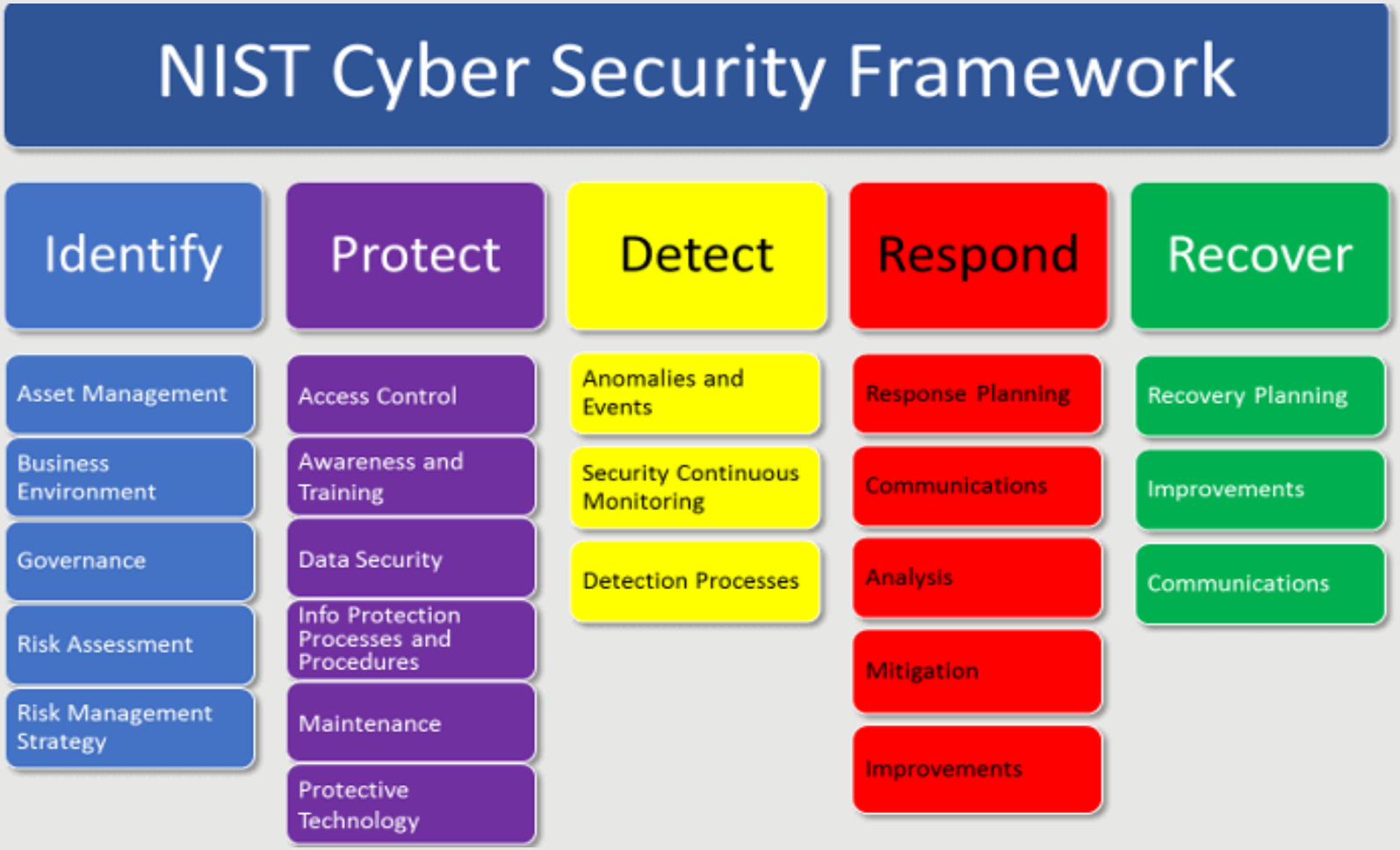
Specific EU Cyber Security standard relevant for the Energy Sector : ISO 27019 (additional controls)

- **Central and distributed process control**, monitoring and automation technology, and operational systems such as programming and parameterization devices;
- **Digital controllers and automation components** such as control and field devices or Programmable Logic Controllers (PLCs), including digital sensors and actuators;
- **Communication technology** used in process control e.g. networks, telemetry, telecontrol applications and remote control technology;
- **Advanced Metering Infrastructure** (AMI) components e.g. smart meters;
- **Digital protection and safety systems** e.g. protection relays, safety PLCs, emergency governor mechanisms;
- **Energy management systems** e.g. Distributed Energy Resources (DER) and electric charging infrastructures in homes and industrial situations;
- **Distributed components of smart grid** environments e.g. in energy grids, homes and industry.

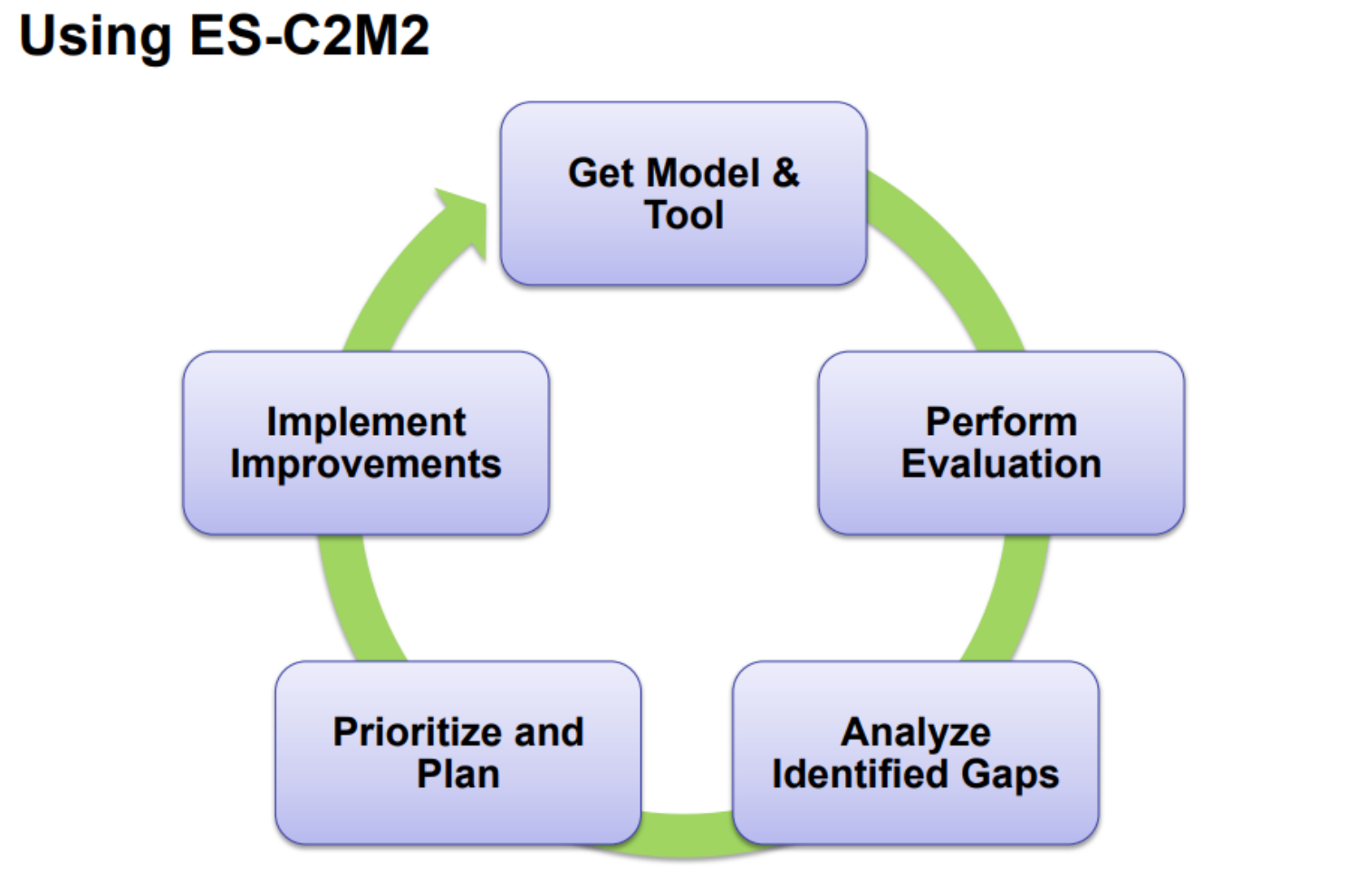
Specific global Cyber Security standard relevant for the Energy Sector : ISA / IEC 62443 (IACS controls)



Specific US Cyber Security standard relevant for the Energy Sector : NIST Cyber Security Framework



Specific US Cyber Security standard relevant for the Energy Sector : Cybersecurity Capability Maturity Model



International good practices from EU member states

	Austria	Croatia	Georgia	Germany	Italy	Netherlands	Portugal
NRA Energy	E-Control	HERA	DEA	Federal Network Agency	ARERA	ACM	ERSE
NRA Cyber Sec	Federal Chancellery	HAKOM		BSI	DIS	AP, ACM	
NCA Cyber Sec	Federal Chancellery	Ministry of Environment & Energy, ZSIS	NSC	BSI	DIS	NCSC	NCSC
National Cyber Security Strategy	✓	✓	✓	✓	✓	✓	✓
National Cyber Security Policies	✓		✓	✓	✓	✓	✓ (not enforced)
National Cyber Security Policies for the Energy Sector	✓			✓		✓	
Smart metering requirements	✓			✓	✓	✓	
Implemented security standards			ISO 27001 ISO 27002 ISO 15408-1	ISO 27001 ISO 27002 ISO 27019	ISO27001 NIST FW (custom.)	ISO27001 ISO27002 ISO27019 IEC62443 ISF GP	ISO27001 NIST FW

International good practices from EU member states

	Austria	Croatia	Georgia	Germany	Italy	Netherlands	Portugal
NRA Energy	E-Control	HERA	DEA	Federal Network Agency	ARERA	ACM	ERSE
NRA Cyber Sec	Federal Chancellery	HAKOM		BSI	DIS	AP, ACM	
NCA Cyber Sec	Federal Chancellery	Ministry of Environment & Energy, ZSIS	NSC	BSI	DIS	NCSC	NCSC
National Cyber Security Strategy	✓	✓	✓	✓	✓	✓	✓
National Cyber Security Policies	✓		✓	✓	✓	✓	✓ (not enforced)
National Cyber Security Policies for the Energy Sector	✓			✓		✓	
Smart metering requirements	✓			✓	✓	✓	
Implemented security standards			ISO 27001 ISO 27002 ISO 15408-1	ISO 27001 ISO 27002 ISO 27019	ISO27001 NIST FW (custom.)	ISO27001 ISO27002 ISO27019 IEC62443 ISF GP	ISO27001 NIST FW

Information Sharing and Analysis Center (ISAC)

Information Sharing and Analysis Center (ISAC)

Recommendations (summary)

1. Appoint the **Regulatory Authority** role to the current **State Electricity Regulatory Commission.**
2. Initiate an independent **State Energy Cybersecurity Competent Authority** that can play an advisory- and supporting role.
3. Initiate a **State Energy Cybersecurity Incident Response Team** unit.
4. Set up a **State Energy Cybersecurity Strategy** led by an **Executive Cyber Security Board** that consists of key players from government, industry and individuals.
5. Join the European CSIRT network to create a broader network of partners and collection of (threat) information
6. Create a list of **Operators of Essential Services (OES)** to identify who must comply with the European Cybersecurity regulations.
7. Set up a **BiH State Energy ISAC** to collaborate under public-private-partnership (PPP) and share valuable information on IT/OT vulnerabilities, threats and incidents according to Traffic Light Protocol (TLP) protocol.
8. Contact the EnC and/or EE-ISAC for advice and support in setting up an ISAC.

THANK YOU FOR YOUR ATTENTION!

USAID Energy Policy Activity (EPA)

Ferhadija 19, Sarajevo, BiH

P. +387 33 251 820 / F. +387 33 251 829

info@usaidepa.ba / usaidepa.ba

Johan Rambi : RambiCo
Telephone : +316 11879945
E-mail : info@rambico.com

USAID FROM THE AMERICAN PEOPLE | ENERGY POLICY ACTIVITY