CYBERSECURITY RISK MANAGEMENT WITH HARDWARE/ SOFTWARE VENDORS

May 9, 2024

USAID JUST AND SECURE ENERGY TRANSITION PROGRAM

TODAY

- Vendor negotiations
- Implementation risk management
- Vendor management
- Vendor offboarding

USAID FROM THE AMERICAN PEOPLE ENERGY BRIDGE

USEA United States Energy Association

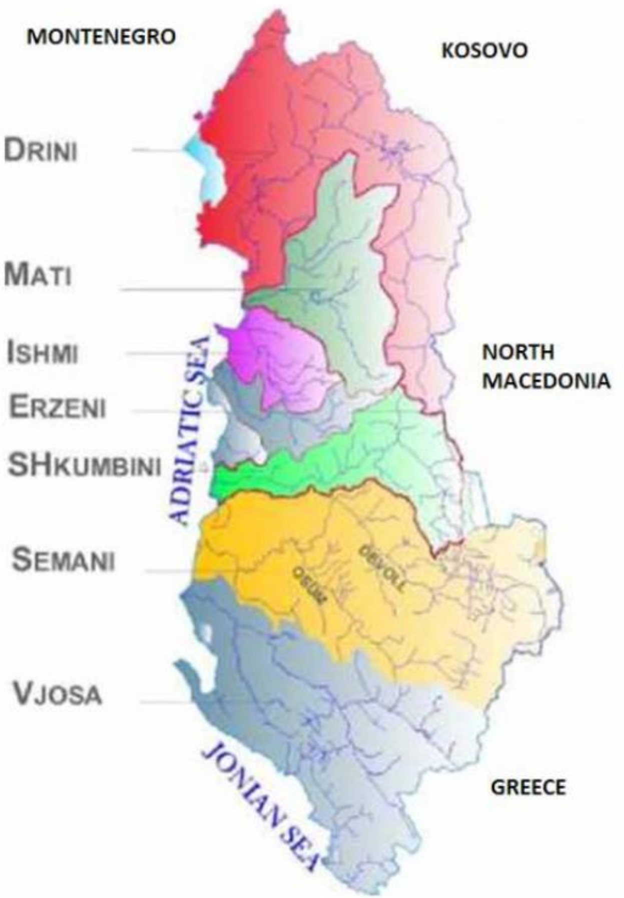
KESH ENERGY OF ALBANIA

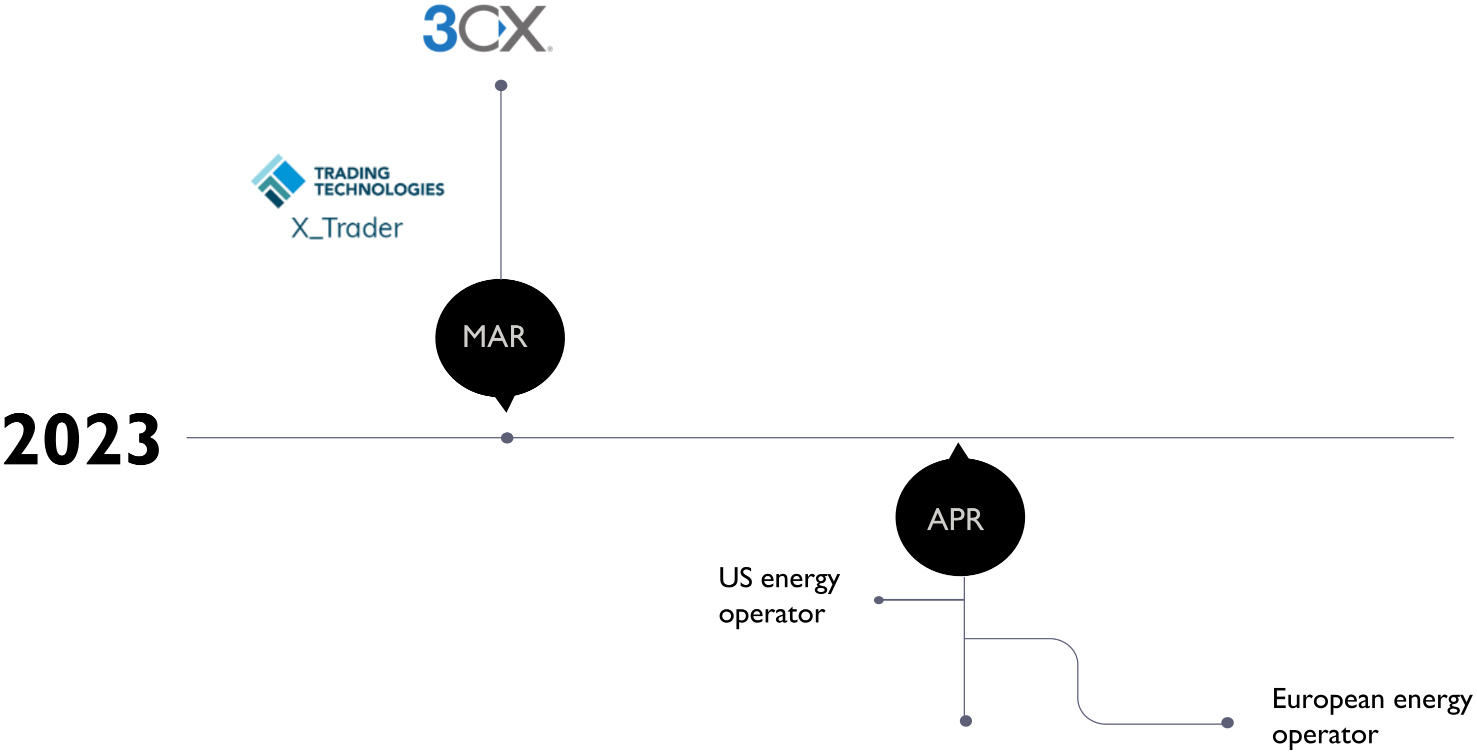
CATALISTO

KESH

ENERGY OF ALBANIA

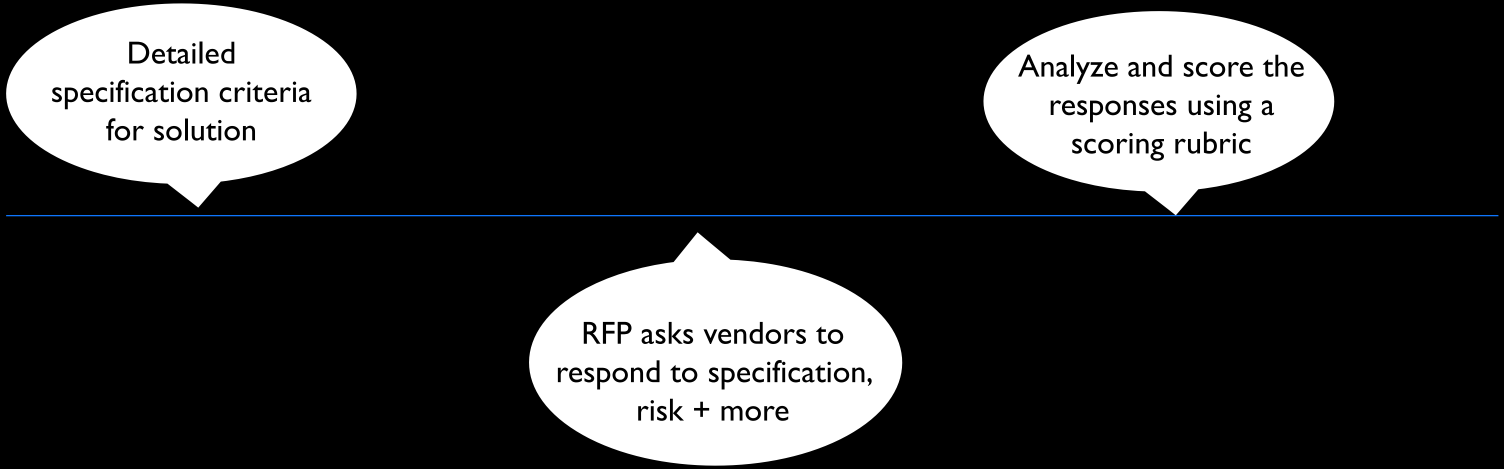
- Critical infrastructure operator
- Largest power producer in Albania (~80% of national generation capacity)
- ~700 employees
- Responsible for energy grid balancing and auxillary services
- Strong reliance on hydroelectric power
- Legacy infrastructure
- Resource constrained





3CX
TRADING TECHNOLOGIES
X_Trader
MAR
2023
APR
US energy operator
European energy operator

KESH PROGRAM



Detailed specification criteria for solution

RFP asks vendors to respond to specification, risk + more

Analyze and score the responses using a scoring rubric

RESPONSE PACKAGES

1. ***Vendor Details:***
   - Ask for details of 3rd party providers/ outsourcing used to deliver the software to you.
   - Make sure you know the name, email and contact number of their CISO

2. ***Technical Solution/ Details:***
   - Solution Description
   - Solution Architecture (needs, cloud based etc., compatibility, opensource/community-based resources)
   - Integration/ Data Collection: Ingesting from where? Integrating to where?
   - Data Storage: Where is it? How long is data kept? Backups of data (and system configurations)?
   - Authentication: MFA for administrators, 2FA for other users? Integration with AD/ SSO?

RESPONSE PACKAGES

3. Cybersecurity Questions:

1. Do you have any security related certifications/ standards you commit to (eg ISO27001, SOC Type II, NIST 800-171, CMMC etc.) and if so describe whether you are independently audited to the standard or self-certified to that standard.

2. How many successful cybersecurity attacks has your organization experienced in the last 2 years? Successful means the attacker was able to gain unauthorized access to systems or information (including solution source code).

3. When was the last time your technical solution was manually penetration tested? (meaning human specialists were used to systematically identify vulnerabilities, navigate the application/ system and attempt to exploit vulnerabilities)

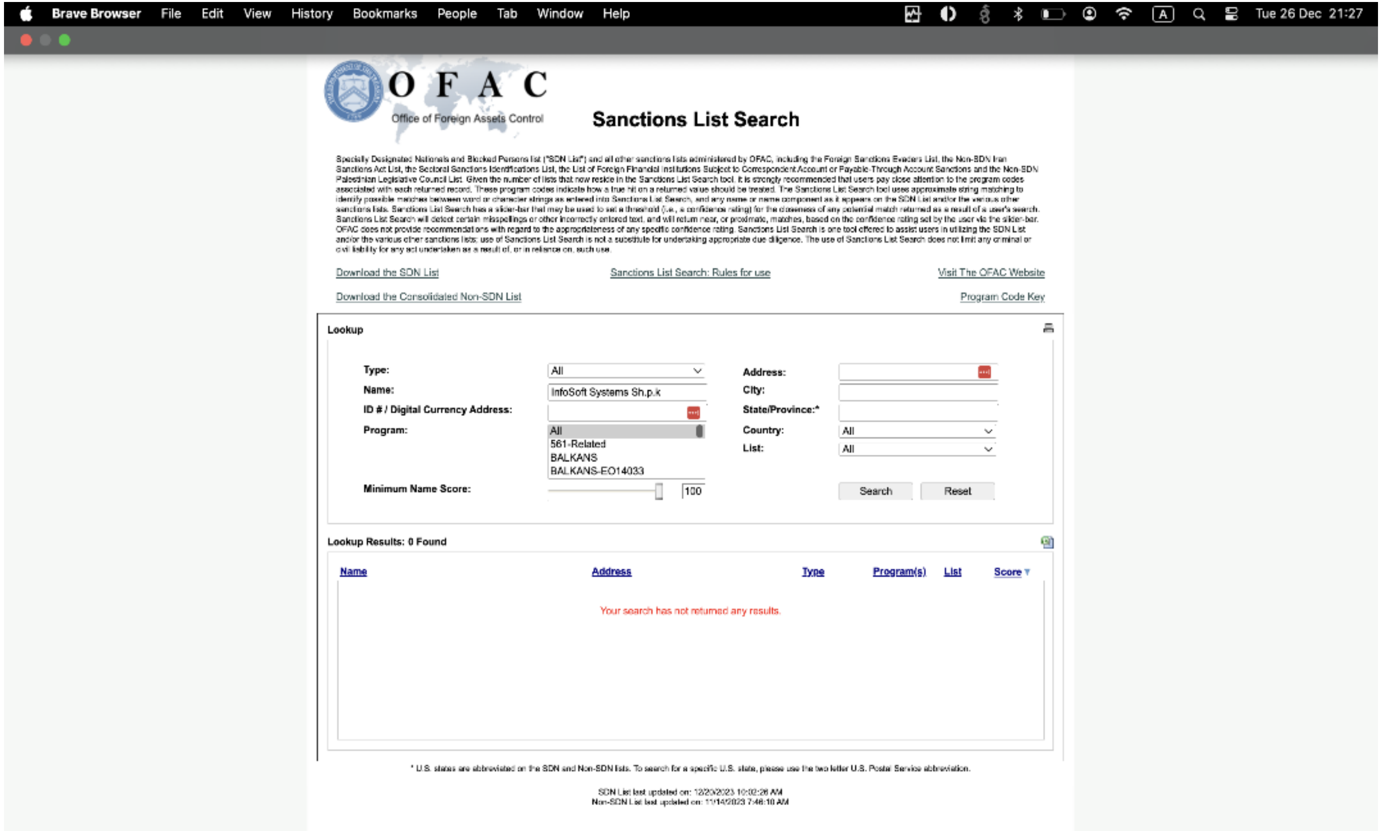
RESPONSE PACKAGES

4. When was the last time your organization was manually penetration tested? (meaning human specialists were used to systematically identify vulnerabilities, navigate the application/ system and attempt to exploit vulnerabilities)

5. Will you agree to disclose the name, nationalities and countries of residence of all personnel involved in implementation of the solution on our systems (that are of national importance)?

6. Will you agree to sign a mutual NDA with the operator to ensure any information disclosed to you during implementation or otherwise is kept in strict confidence?

COMPLIANCE CHECKS



Brave Browser File Edit View History Bookmarks People Tab Window Help
Tue 26 Dec 21:27
O F A C
Office of Foreign Assets Control

Sanctions List Search

Specially Designated Nationals and Blocked Persons list ("SDN List") and all other sanctions lists administered by OFAC, including the Foreign Sanctions Evaders List, the Non-SDN Iran Sanctions Act List, the Sectoral Sanctions Identifications List, the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions and the Non-SDN Palestinian Legislative Council List. Given the number of lists that now reside in the Sanctions List Search tool, it is strongly recommended that users pay close attention to the program codes associated with each returned record. These program codes indicate how a true hit on a returned value should be treated. The Sanctions List Search tool uses approximate string matching to identify possible matches between word or character strings as entered into Sanctions List Search, and any name or name component as it appears on the SDN List and/or the various other sanctions lists. Sanctions List Search has a slider-bar that may be used to set a threshold (i.e., a confidence rating) for the closeness of any potential match returned as a result of a user's search. Sanctions List Search will detect certain misspellings or other incorrectly entered text, and will return near, or proximate, matches, based on the confidence rating set by the user via the slider-bar. OFAC does not provide recommendations with regard to the appropriateness of any specific confidence rating. Sanctions List Search is one tool offered to assist users in utilizing the SDN List and/or the various other sanctions lists; use of Sanctions List Search is not a substitute for undertaking appropriate due diligence. The use of Sanctions List Search does not limit any criminal or civil liability for any act undertaken as a result of, or in reliance on, such use.

Download the SDN List | Sanctions List Search: Rules for use | Visit The OFAC Website

Download the Consolidated Non-SDN List | Program Code Key

Lookup

Type: All

Name: InfoSoft Systems Sh.p.k

ID # / Digital Currency Address:

Program: All
561-Related
BALKANS
BALKANS-EO14033

Minimum Name Score: 100

Address:

City:

State/Province:*

Country: All

List: All

Search Reset

Lookup Results: 0 Found

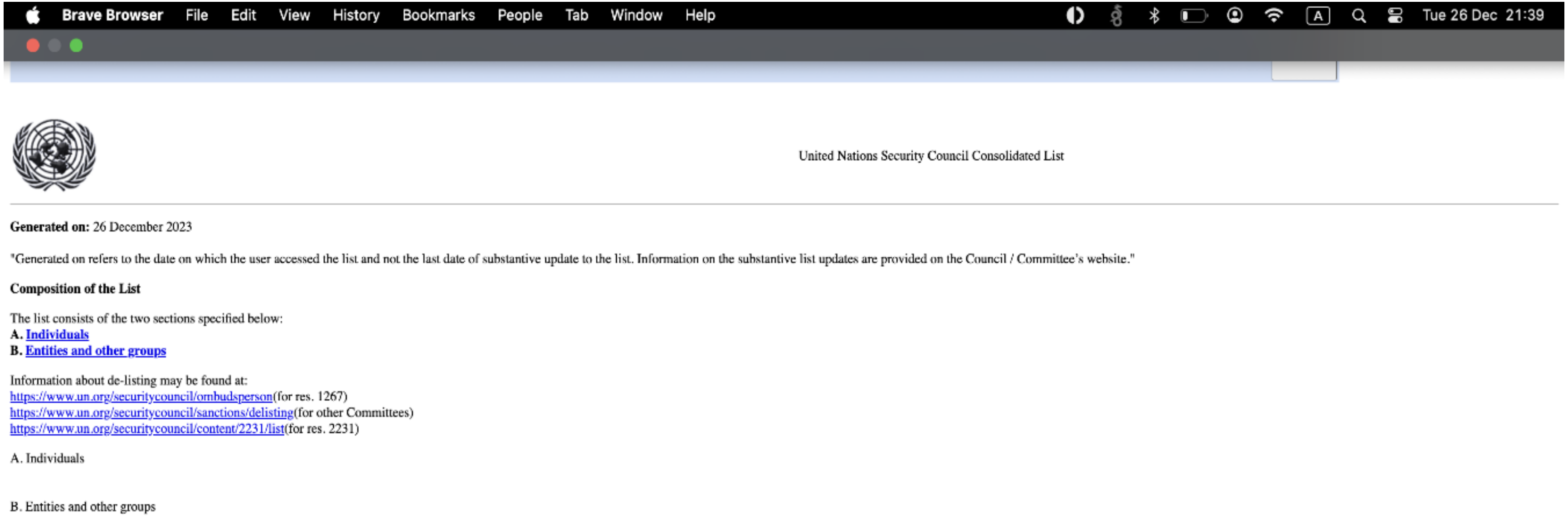
Name	Address	Type	Program(s)	List	Score

Your search has not returned any results.

* U.S. states are abbreviated on the SDN and Non-SDN lists. To search for a specific U.S. state, please use the two letter U.S. Postal Service abbreviation.

SDN List last updated on: 12/20/2023 10:02:26 AM
Non-SDN List last updated on: 11/14/2023 7:46:10 AM

COMPLIANCE CHECKS



United Nations Security Council Consolidated List

Generated on: 26 December 2023

"Generated on refers to the date on which the user accessed the list and not the last date of substantive update to the list. Information on the substantive list updates are provided on the Council / Committee's website."

Composition of the List

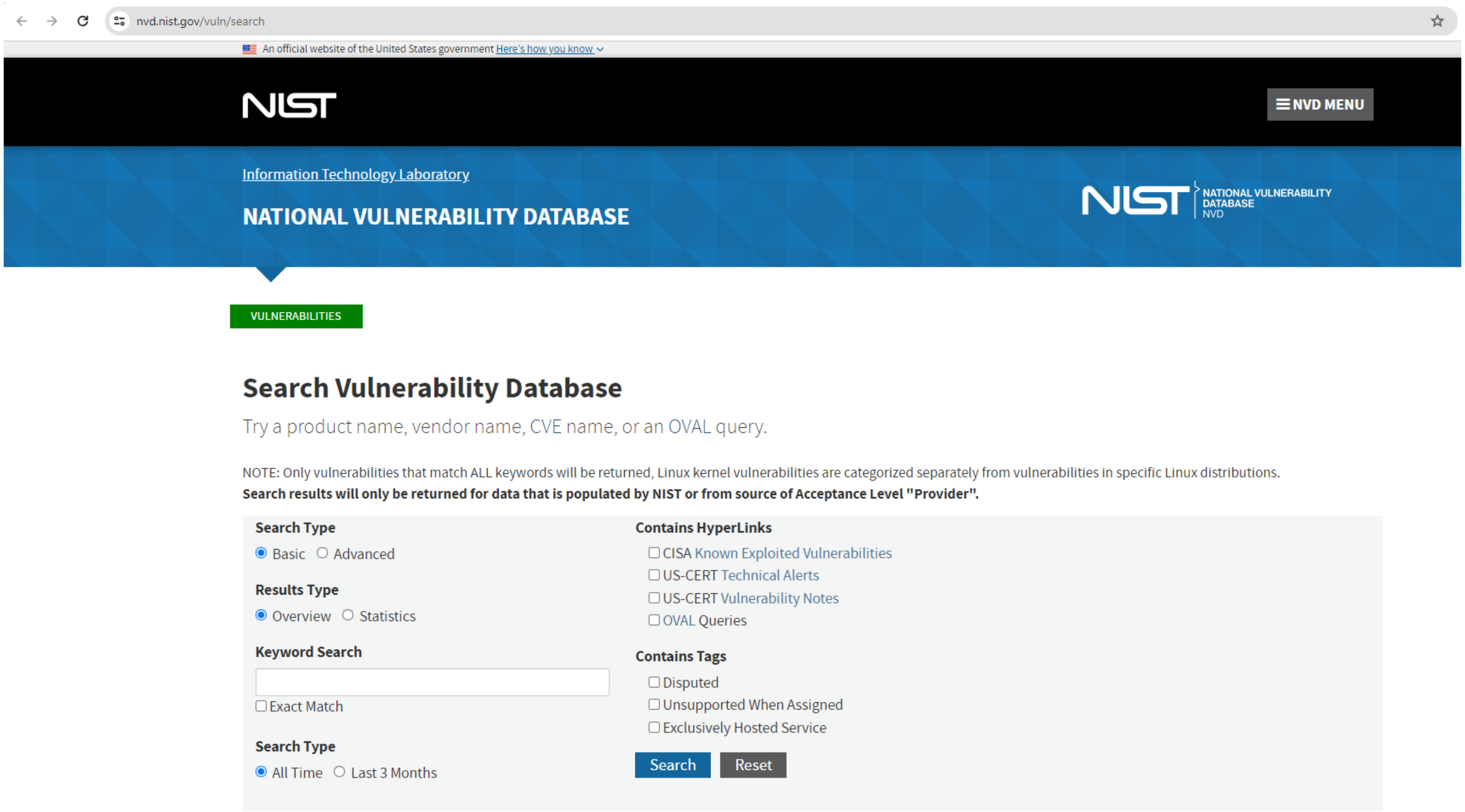
The list consists of the two sections specified below:
A. **Individuals**
B. **Entities and other groups**

Information about de-listing may be found at:
https://www.un.org/securitycouncil/ombudsperson(for res. 1267)
https://www.un.org/securitycouncil/sanctions/delisting(for other Committees)
https://www.un.org/securitycouncil/content/2231/list(for res. 2231)

A. Individuals

B. Entities and other groups

NATIONAL VULNERABILITY DATABASE (NIST)



nvd.nist.gov/vuln/search

An official website of the United States government Here's how you know

NIST

☰ NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

Search Vulnerability Database

Try a product name, vendor name, CVE name, or an OVAL query.

NOTE: Only vulnerabilities that match ALL keywords will be returned, Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions.
Search results will only be returned for data that is populated by NIST or from source of Acceptance Level "Provider".

Search Type

● Basic ○ Advanced

Results Type

● Overview ○ Statistics

Keyword Search

□ Exact Match

Search Type

● All Time ○ Last 3 Months

Contains HyperLinks

□ CISA Known Exploited Vulnerabilities
□ US-CERT Technical Alerts
□ US-CERT Vulnerability Notes
□ OVAL Queries

Contains Tags

□ Disputed
□ Unsupported When Assigned
□ Exclusively Hosted Service

Search Reset

5/22/2024

NEGOTIATIONS

1. Clarify with vendor based on their responses.
2. Do reference checks and ask references about any issues/ risks
3. Do a vendor risk assessment
4. Get the vendor to commit (in the contract) to certain changes to manage risk
5. Rewrite your specifications and incorporate it into your statement of work

VENDOR RISK ASSESSMENT

Cybersecurity Risk

CS1 Does the organization have a robust cybersecurity strategy, awareness and controls in place?

CS2 Are their developers / operations located in potentially compromised / adversarial jurisdictions?

Compliance Risk

CO2 GDPR, PCI, FARs/ DFARs/ AIDAARs, Do they engage in misleading or deceptive practices, does they have a sound set of policies and procedures, how have they performed in recent exams or audits?

Reputational Risk

RP1 Risk that we would attract a negative public of customer opinion by working with this vendor? Does the vendor have a history of unresolved customer complaints? Have they received any negative press?

Credit/ Financial Risk

FI1 Is the vendor excessively expensive (constraining revenue)

FI2 Does the vendor have a risk of non-performance due to financial condition?

FI3 Is there a risk of foreign currency translation, price fluctuations, liquidity issues?

Operational Risk

OP1 To what extent will vendor shutdown impact our day to day operations? Does the vendor have a business continuity and disaster recovery plan?

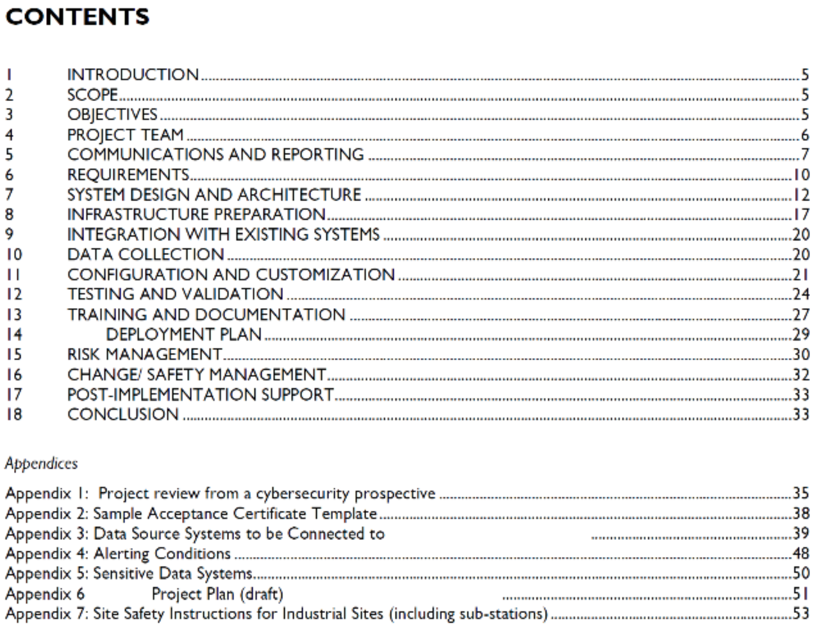
Strategic Risks

SR1 Is there are risk that this vendor will make business decisions that are not aligned with our strategic operations?

Transaction Risks

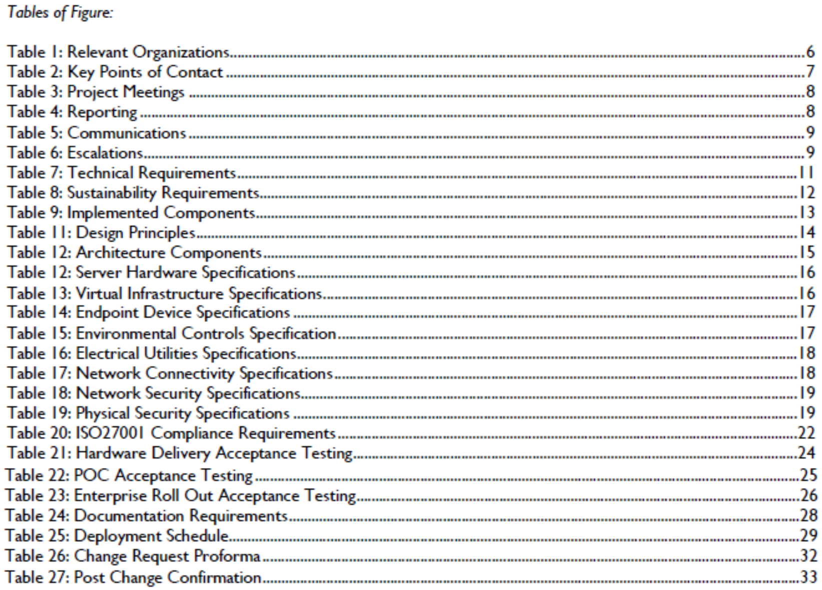
TR1 Is there a risk that the vendor will not be able to perform due to inadequate capacity, technological failure, human error or fraud?

IMPLEMENTATION PLANS



CONTENTS

Appendices



Tables of Figure:

IMPLEMENTATION RISK: CYBERSECURITY SPECIFIC

Methodology

Research went through two steps:

- Search based on company name, including:
  - Geopolitical factors
  - Cybersecurity risks
    - Data Breaches
    - Exploits
  - Certifications about products and compliant with standards used

- Analyze about network topology and proposed infrastructure
  - What data is gathered?
  - Is data sent to a specific server or everything is intranet?
  - What ports and protocols are used?

Assessment Summary

Risk Level	Nr. of risks
Low	3
Medium	3
High	5

1.Tabela 1 – Risk summary

IMPLEMENTATION RISK: CYBERSECURITY SPECIFIC

3.1 Analysis about network topology and proposed infrastructure

Based on the information provided, there are several potential cyber threats that could affect the infrastructure. These include unauthorized access to the system, data breaches, and malware, man-in-the-middle attacks etc. During the analyses of the technical proposal, we have identified some findings (but not limited to) that might be potential risk for the security of infrastructure as below:

- **No secure perimeter.** The communication outside of the infrastructure is not secure because no firewall is mentioned in the proposal. This is a potential risk for the attackers to gain access to inside infrastructure.

- **Lack of segmentation.** There is no network segmentation between different services and devices in the PV network. If one of the devices is compromised it would be escalated for all network and devices.

- **Remote access for maintenance for XXXXX.** The whole infrastructure is predicted to be maintained remote, so it is a big risk for the exposure to internet.

- **Connection to Cloud.** Risk of data stored in cloud and exposure to internet, and whether an attack can be escalated to the SCADA system?

IMPLEMENTATION RISK: CYBERSECURITY SPECIFIC

3.2 Recommendations

To mitigate these risks, a comprehensive security design should be implemented in order to reduce potential cyber threats to the infrastructure.

The following measures can be taken:

- **Access controls:** Access to the system should be restricted to authorized personnel only. This can be achieved through the use of strong passwords, two-factor authentication, and access controls; Restrict access to the system to only authorized personnel and implement role-based access controls to limit access to sensitive data.

- **Data encryption:** Sensitive information should be encrypted to protect it from unauthorized access. This can be achieved through the use of secure protocols such as SSL/TLS and VPNs. That's important to the connection to cloud also if applicable.

- **Regular backups:** Regular backups of critical data should be taken to ensure that data can be restored in the event of a cyber-attack or system failure. These backups should be stored in a secure location and tested regularly to ensure that they can be restored successfully. Backups should include also configurations of devices and machines.

IMPLEMENTATION RISK: CYBERSECURITY SPECIFIC

- **Software updates:** All software and firmware should be kept up to date with the latest security patches and updates. This will help to prevent known vulnerabilities from being exploited by cyber attackers.

- **NextGen Firewalls:** Firewalls can be used to monitor and control network traffic to and from the infrastructure. This can help to prevent unauthorized access and data breaches. Firewalls will also support OT protocols such ###, or ###.

- **Intrusion detection and prevention IDS/IPS:** Intrusion detection and prevention systems can be used to monitor the infrastructure for potential cyber threats and take action to prevent them. This can also be done from NextGen Firewalls.

- **Network segmentation:** The infrastructure should be segmented into different networks to limit the potential impact of a cyber-attack and to lower the attack surface. This can help to prevent an attacker from gaining access to the entire system. This can also be done from NextGen Firewalls (depending on configuration).

- **Antivirus system, EDR or XDR** are advanced threat detection and response solutions that provide real-time monitoring and analysis of system activity to detect and respond to cyber threats. EDR focuses on endpoint devices, while XDR extends the scope to include network and cloud environments.

IMPLEMENTATION RISK: CYBERSECURITY SPECIFIC

- **Continuous monitoring:** Continuous monitoring of the infrastructure can help to detect potential cyber threats in real-time. This can include the use of SIEM systems, network monitoring tools, and other monitoring tools.

- **Secure remote access with "zero trust principle”.** In case of maintaining the infrastructure from outside it is recommended to also a jump server to monitor the remote session and to record it, also remote session will be on request and not always opened.

- **Hardening.** It is necessary to have a hardening process for all devices including operating systems that will be used and network devices. CIS benchmarks are recommended for OT infrastructure.

- **Security audits and Pen-Test:** Regular security audits should be conducted to identify and address any vulnerabilities in the system.

POST IMPLEMENTATION

Update

- your asset inventory
- your systems inventory
- your data inventory
- your business continuity plan / incident response processes / emergency contact list
- Annual risk audits/ updates with vendor?

OFFBOARDING

- Do you understand the uninstall process?
  - Can you simply delete it?
  - How long does it take to decommission and recommission to another provider?
- How is data being stored (retention policy) within your company?
- How is data being destroyed at the vendor site?
- Update all your inventories

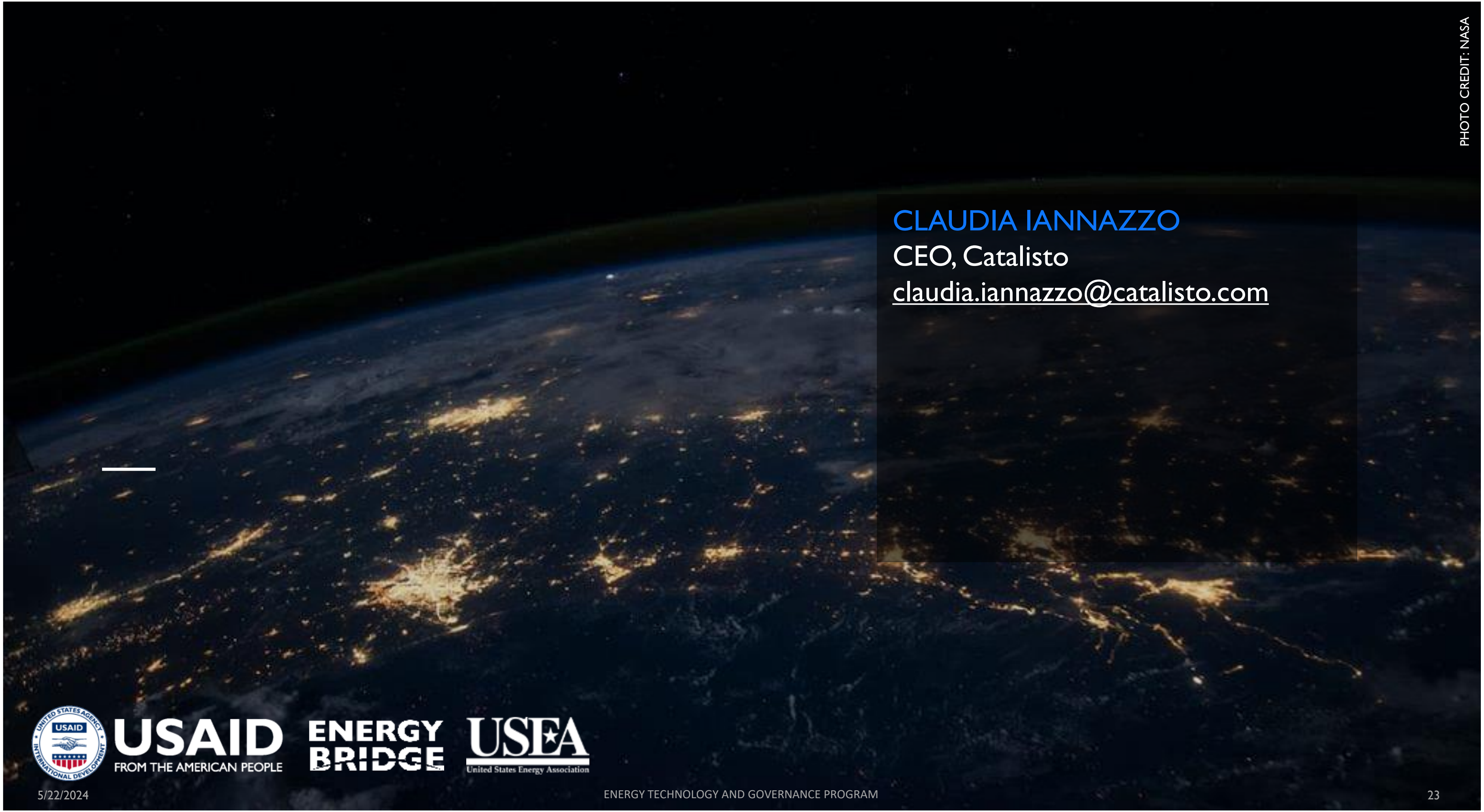


PHOTO CREDIT: NASA

CLAUDIA IANNAZZO

CEO, Catalisto

claudia.iannazzo@catalisto.com

USAID FROM THE AMERICAN PEOPLE ENERGY BRIDGE USEA United States Energy Association

ACRONYMS USED

APT	Advanced persistent threat (actor)
CIS	Centre for Internet Security
GDPR	Global Data Protection Regulations
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	International Standards Organization (standard)
IT	Information Technology
KESH	Korporata Elektroenergjetika Shqiptare (Albanian Energy Corporation)
NIST	National Institute of Standards and Technology
OT	Operational Technology
PCI	Payment Card Industry (standards)
SIEM	Security Incident and Event Management
USAID	United States Agency for International Development
USEA	United States Energy ASsociation