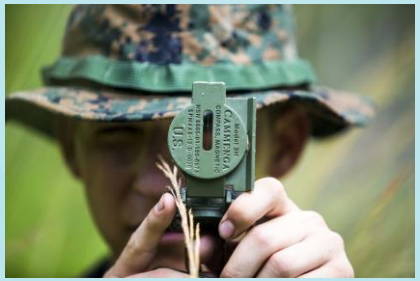
SOFTWARE ASSURANCE GUARDIAN™ (SAG™)

Never trust software, always verify and report! ™



CONFIDENTIAL INTRODUCTION

PROPOSED METHOD TO COMPLY WITH FERC ORDER 850 AND NERC SUPPLY CHAIN STANDARDS FOR SOFTWARE INTEGRITY AND AUTHENTICITY VERIFICATION

JULY 25, 2019

R E A

RELIABLE ENERGY ANALYTICS LLC

NOTICE

NOTE: The materials contained in this presentation describe **PATENT PENDING TECHNOLOGIES** that are the intellectual property of Reliable Energy Analytics LLC and have been designed to protect the integrity of the Bulk Electric System Critical Infrastructure and its software components. All of the materials presented and discussed as part of this overview presentation are the intellectual property of Reliable Energy Analytics LLC. None of the materials presented and/or discussed during this presentation, provided in both written and oral forms, may be shared beyond the audience receiving this material, without the written consent of Reliable Energy Analytics LLC.

NERC CIP-013.1 AND CIP-010-3 REQUIREMENTS FOR SOFTWARE INTEGRITY AND AUTHENTICITY **IN SCOPE FOR SAG**

Standard/Requirement	Description	Required Evidence
CIP-013-1 R1.1.2.5	(1.2) One or more process(es) used in procuring BES Cyber Systems that address the (1.2.5) Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System	Evidence shall include one or more documented supply chain cyber security risk management plan(s)
CIP-013-1 R2	Each Responsible Entity shall implement its supply chain cyber security risk management plan(s) specified in Requirement R1	Evidence shall include documentation to demonstrate implementation of the supply chain cyber security risk management plan
CIP-010-3 R1 Part 1.6	… when the method to do so is available to the Responsible Entity from the software source: 1.6.1. Verify the identity of the software source; and 1.6.2. Verify the integrity of the software obtained from the software source.	may include, but is not limited to a change request record that demonstrates the verification of identity of the software source and integrity of the software was performed prior to the baseline change or a process which documents the mechanisms in place that would automatically ensure the identity of the software source and integrity of the software.

SOFTWARE VERIFICATION CIP-010-3 (PAGE 36)

The concept of software verification (**verifying the identity of the software source and the integrity of the software obtained from the software source**) is a key control in preventing the introduction of malware or counterfeit software. This objective is **intended to reduce the likelihood that an attacker could exploit legitimate vendor patch management processes to deliver compromised software updates or patches to a BES Cyber System.**

NERC/NATF GUIDANCE ORDER 850

Endorsed Implementation Guides

Cyber Security Supply Chain Risk Management Plans

CIP-010-3 R1.6 Software Integrity and Authenticity (NATF)

Executive Order 13873 of May 15, 2019

Securing the Information and Communications Technology and Services Supply Chain

Implementation Guidance for Verifying the Identity of the Software Source and the Integrity of the Software with a Single Method

Some methods may complete both the verification of the identity of the software source and the verification of the integrity of the software obtained from the software source. Validation of digitally signed software is an example of a method that accomplishes both obligations required in CIP-010-3 Requirement 1, Part 1.6. Further, some processes may handle this in an automated fashion. One example of this is the Microsoft update process using Windows Server Update Services (WSUS) as described in the article found at the following link:

https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx

IS DIGITAL SIGNATURE VERIFICATION ALONE SUFFICIENT TO ESTABLISH TRUST IN A SOFTWARE OBJECT

- There are numerous cases where a digitally signed object should never have been trusted
- ASUS March 29, 2019

  As *Motherboard* reported earlier this week, researchers at Kaspersky discovered that malicious hackers had **successfully planted malware posing as an official ASUS security update** onto ASUS's servers **and signed it with two of the company's legitimate digital certificates.**

- COMODO Fraudulent Certificates

  Microsoft is aware of nine fraudulent digital certificates issued by Comodo, a certification authority **present in the Trusted Root Certification Authorities Store, on all supported releases of Microsoft Windows** Comodo advised Microsoft on March 16, 2011 that **nine certificates had been signed on behalf of a third party without sufficiently validating its identity.**

- **As indicated in FERC Order 829 at 28 on page 18:**

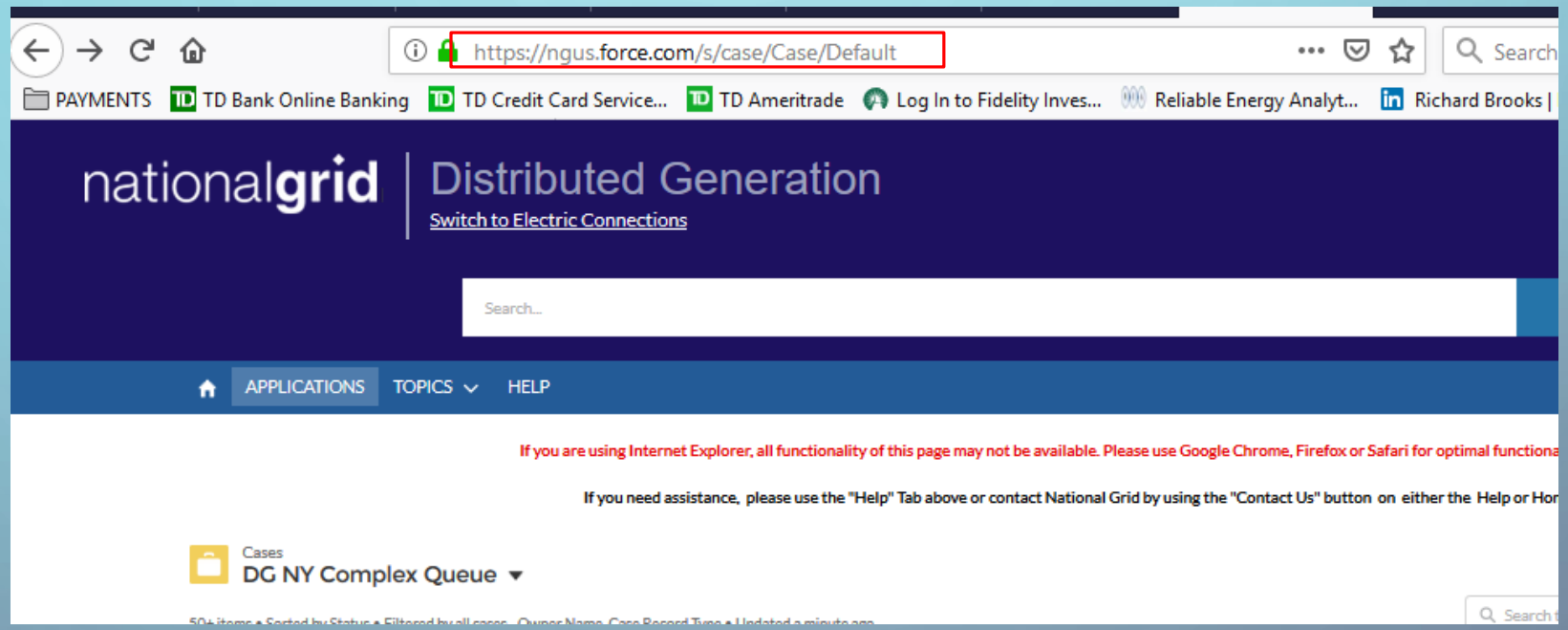
  Peak notes, for example, **that it is possible for a malware campaign to infect industrial control software with malicious code while the product or service is in the control of the hardware and software vendor**, and states that, "[w]ithout proper controls, **the vendor may deliver this infected product or service, unknowingly passing the risk onto the utility industry customer.**"

WHAT HAPPENS WITH UNSIGNED SOFTWARE OBJECTS

- Many software objects are unsigned
  - Commercial products, i.e. Oracle, Microsoft, etc.
  - Numerous GitHub objects
  - Shareware and Open Source software
- Should a Responsible Entity install them anyway?
- Software risks are found in lots of places!

CLOUD BASED SOFTWARE IS GROWING ACCEPTANCE IN ENERGY – FORCE.COM

National Grid is committed to keeping stakeholders informed of the Cluster Study process and progress. National Grid already has held several stakeholder informational meetings, and plans to hold another one in August 2019 at which preliminary study findings from Part 1 of the Cluster Study will be provided. Additionally, a webpage, which can be found at (https://ngus.force.com/s/article/Affected-Substations), has been created where stakeholders can



https://ngus.force.com/servlet/servlet.FileDownload?file=0150W00000F7tR5

OVERARCHING GOAL OF SAG METHODS

- To fulfill FERC Order 850's stated objective at 80 on page 49 (below) by implementing appropriate mitigating actions to meet the three specific in-scope requirements identified on slide 3, pertaining to software integrity and authenticity verification prior to making any changes to the baseline configuration of a BES Cyber Asset:

  The security objective of the supply chain risk management Reliability Standards is to "ensure that [r]esponsible [e]ntities consider the security, integrity, quality, and resilience of the supply chain, and take appropriate mitigating action …

SAG PHILOSOPHY: **NEVER TRUST SOFTWARE, ALWAYS VERIFY AND REPORT!**

- The philosophy behind SAG's design is based on the same in-depth level of due diligence a Company might apply when hiring a new employee to work in the Control Room; After all that's what many BES software applications do – they work for the Control Room
- Provide Responsible Entities with the most timely, accurate information available to make a risk based decision on the trustworthiness of a software object to perform, as expected, in it's BES role
- SAG makes every effort to ensure that a thorough "background check" is performed to determine the integrity and authenticity of a software object, using the best practices available, on an on-going basis
- Produce a SAGScore indicating the statistical level of trustworthiness, based on all of the information collected during SAG Software execution. The score ranges from 0 to 1 where 0 indicates no trust and 1 indicates complete trust; a software object with a SAGSCore less than .85 should not be trusted/installed in a BES Cyber Asset
- And when a "bad actor" is identified, SAG get's the word out as soon as possible so that other BES operators can be made aware of the elevated risk associated with a software object

SAG SOFTWARE VERIFICATION OBJECTIVES

- Implement a risk assessment based approach to verify software integrity and authenticity
- Apply cryptographic (i.e. PKI) verification methods for software object integrity and authenticity, when available
- Perform a virtual online "background check" pertaining to the authentication and integrity of supply chain entities, locations and software objects and provide this information to the Responsible Entity during SAG Software execution to aid in their risk assessment decision
- Statistically produce a SAGScore to indicate the confidence level of trust based on all the collected information
- Present the SAGScore and sufficient information to aid a Responsible Entity in deciding to trust, or not trust the entities, locations and integrity affiliated with a software object so that a PASS or FAIL decision can be assigned
- All of the contextual information, background check information and responses from the Responsible Entity are stored for posterity in a tamperproof record for further examination by auditor or forensic teams
- Provide Responsible Entities with a "Proof of Verification" that may be saved in a Change Management System or other system of record for logging changes to BES systems
- Record sufficient information in a central "List of Trusted Software" that may be presented to other Responsible Entities when they are deciding to trust/not trust a software object that has been verified by other Responsible Entities.
- Facilitate the reporting of "attempt to compromise" cyber security incidents with NERC E-ISAC and NCCIC, when appropriate to do so

WHAT IS SOFTWARE INTEGRITY

- According to NIST SP800-161

  *"Integrity is focused on ensuring that the ICT products or services in the ICT supply chain are genuine, unaltered, and that the ICT products and services **will perform according to acquirer specifications and without additional unwanted functionality**."*

- According to SAFECode's **The Software Supply Chain Integrity Framework**

  *"Software integrity is an element of software assurance. SAFECode defines Software Assurance as "**confidence that software, hardware and services are free from intentional and unintentional vulnerabilities and that the software functions as intended.**"*

- Microsoft identifies broad classes of threats to software integrity:

  - *Broad classes of software integrity threats in an operational environment include (but are not limited to): **Malicious software inserted into a production environment by a staff member***

SAG SOFTWARE INTEGRITY VERIFICATION OBJECTIVES

- Contains no known malware or viruses
- Determine if a software object was obtained from a trustworthy location
- Determine if a software object was obtained from trustworthy supply chain entities
- Is unaltered from it's original intended contents, as provided by a trustworthy software source originator or software source using cryptographic methods where possible
- Contains no recorded/known vulnerabilities or reports of suspicious activity (i.e. Bitcoin mining)
- Determine if other parties have assigned a passing grade for integrity verification of a specific software object
- Ensure that Responsible Entities are informed of any integrity related risks pertaining to the route used to obtain a software object, i.e. did it go through a system in Iran?

WHAT IS SOFTWARE AUTHENTICITY

- FERC Order 829 directed NERC to:

  address verification of: (1) the identity of the software publisher for all software and patches that are intended for use on BES Cyber Systems; (Order 829 page 48)

- NERC CIP-010-3 states in R1 requirement 1.6.1:

  1.6.1. Verify the identity of the software source;

- NERC CIP-013-1 states in R1 requirement 1.2.5

  Verification of software integrity and authenticity of all software and patches provided by the vendor for use in the BES Cyber System

- Implementation guidance produced by NATF, available from NERC states:

  Verify software authenticity to ensure that the software being installed in the BES Cyber System is from a legitimate source.

- Are "software publisher" (Order 829), "software source" (CIP 010-3), "vendor" (CIP-013-1) and "legitimate source" (NATF CIP-010-3 Guidance), all referring to the same entity?

FERC ORDER 850 GUIDANCE: PAGE 47 AT 78

The Supplemental Materials for Reliability Standard CIP-013-1 explain the **meaning of the term "vendor."** Specifically, the Supplemental Materials state that **a vendor "is limited to those persons, companies, or other organizations with whom the [r]esponsible [e]ntity, or its affiliates, contracts with to supply BES Cyber Systems and related services."**

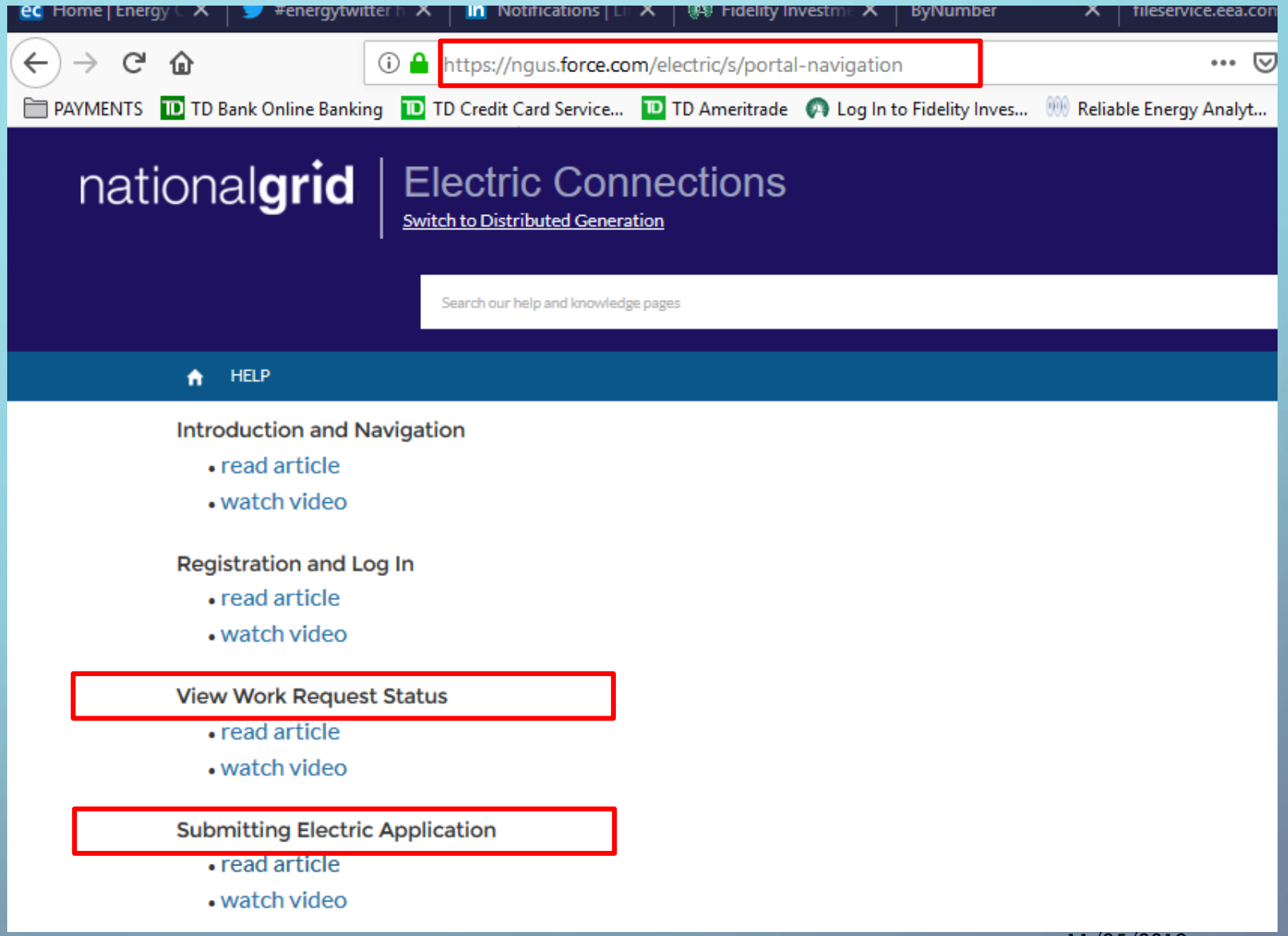
The Supplemental Materials also note that **a vendor, for purposes of the supply chain risk management Reliability Standards, may include: (i) developers or manufacturers of information systems, system components, or information system services; (ii) product resellers; or (iii) system integrators.**

- **There is frequently more than one "vendor", based on this definition, in the software supply chain**

SAG DIFFERENTIATES ENTITIES IN THE SOFTWARE SUPPLY CHAIN ACCORDINGLY

- **Software Source Originator**: Is the entity that authored/published a software object and is the authorized licensor of the software i.e. Microsoft Corp
  - This most likely correlates with (FERC 829) publisher and (CIP-013-1) vendor, but may also correlate with (CIP-010-3) software source
- **Software Source**: Is the entity that made the software object available to a party wishing to utilize the software object, i.e. https://github.com/microsoft
  - This most likely correlates with (CIP 010-3) "software source" and (NATF) "legitimate source", but it could also correlate with (CIP-013-1) vendor
- **Software Source Location**: Physical location where the software object was obtained from, i.e. https://github.com/microsoft/vscode
  - This does not appear to have a direct correlation with other defined entities in FERC Order 850 or 829 nor within NERC standards CIP-013-1and CIP 010-3
- Amazon Example: Malwarebytes Security: Virus Cleaner, Anti-Malware
  - **Download instructions: Open the Amazon Underground** on your device, then go to Menu → My Apps → Cloud → Refresh to see your newly purchased app to download and install.
- NOTE: GitHub is home to over 36 million developers working together.

CLOUD BASED APPLICATION EXAMPLE



SAG SOFTWARE AUTHENTICITY VERIFICATION OBJECTIVES

- SAG authenticity verification is performed for all 3 supply chain entities:
  - **Software Source Originator**
  - **Software Source**
  - **Software Source Location**
- Utilize public key infrastructure (X.509, CRL's, OCSP, etc.), PGP trust chains, etc. to verify the signing party of a software object, when possible, but this is only one step in the process!
- Search for corroborating evidence of an entities proclaimed identity, i.e. NAESB EIR, D&B search, etc.
- Search for known compromises, fraudulent certificate reports and other information that may affect the trustworthiness of an entity
- Determine if an entity has any affiliation with high-risk State actors, i.e. Iran, or known sources of risk, i.e. dropbox

SAG SOFTWARE VERIFICATION PROOF OBJECTIVES

- Produce a tamperproof "record" of the integrity and authenticity background check results along with the Responsible Entities responses and other contextual information, including PASS/FAIL grades, SAGScore and other information obtained during SAG Software execution, i.e. comments supporting a PASS/FAIL decision
- Prevent bad actors from altering the "record" of information that was used to determine the trustworthiness of a software object as other parties may rely on this information during audits and/or forensic inspections relating to a cyber incident

Two out of three organizations fell victim to a cyberattack in 2018

IT managers can't just focus on email and web, however. 23% of attacks got in via a software vulnerability, and 14% via a USB stick or external device. Furthermore, 20% of IT managers didn't know how the most significant attack got in – if you don't know which security door has been left open it's hard to shut it.

Given the variety and complexity of threats, it's not surprising that 86% of respondents say they need greater cybersecurity skills in their organization. Those organizations that had experienced an attack have greater need for cybersecurity expertise than those that hadn't (89% vs. 79%). This could be because they have more security issues that need fixing, or the result of heightened awareness of the complexity of today's attacks.

Source: https://secure2.sophos.com/en-us/security-news-trends/whitepapers/gated-wp/the-impossible-puzzle-of-cybersecurity.aspx

Meet the World's Biggest 'Bulletproof' Hoster

Yalishanda would re-brand and market his pricey bulletproof hosting services under a variety of nicknames and cybercrime forums over the years, including one particularly long-lived abuse-friendly project aptly named **abushost[.]ru.**

In a talk given at the Black Hat security conference in 2017, researchers from Cisco and cyber intelligence firm Intel 471 labeled Yalishanda as one the "top tier" bulletproof hosting providers worldwide, noting that **in just one 90-day period in 2017 his infrastructure was seen hosting sites tied to some of the most advanced malware contagions at the time, including the Dridex and Zeus banking trojans, as well as a slew of ransomware operations.**

Source: https://krebsonsecurity.com/2019/07/meet-the-worlds-biggest-bulletproof-hoster/

2018 NERC COMPLIANCE ISSUES

Focus on Serious Risk Issues

In 2018, NERC filed 12 Full NOPs with a combined penalty amount of $4,279,000. These Full NOPS included 6 serious, 14 moderate, and 15 minimal risk violations. The Full NOPs filed in 2018 included a range of serious risk issues that NERC has identified as potential areas for future focus of ERO Enterprise resources:

• **Multiple instances of noncompliance with CIP standards as a result of issues with implementing new tools and processes**, asset and configuration management, inadequate training and management oversight, **contractor and vendor failures**, failure of situational awareness, development of organizational silos, and **a lack of clearly defined internal policies**;

SUMMARY

- SAG™ provides Responsible Entities of all sizes and skills with the best practices available to verify software integrity and authenticity consistently throughout the BES ecosystem
- A statistically produced SAGScore™ provides Responsible Entities with a confidence level indication of the trustworthiness of a software object to aid in the final decision to PASS or FAIL a software object
- No Responsible Entity should install software without first verifying with SAG™
- ***Never trust software, always verify and report!***™

PROPOSAL

- If you believe the Software Assurance Guardian™ methods and processes presented and discussed during this presentation would help BES responsible entities, especially smaller entities lacking in cybersecurity skills, detect some cyber attacks emanating from the software supply chain and protect the BES from harmful software, then please consider endorsing SAG™ as an acceptable method to comply with FERC Order 850, NERC CIP-013-1 R11.2.5, R2 and CIP-010-3 R1 part 1.6, pertaining to software integrity and authentication verification

NEXT STEPS

- Partner with a software vendor to develop the SAG software programs needed to implement the methods described in the patent application
- There is a lot work to accomplish between now and July 1, 2020; the sooner this work starts, the better the prospects of going live by 7/1/2020

REFERENCES

- Safecode framework: http://safecode.org/wp-content/uploads/2014/06/SAFECode_Supply_Chain0709.pdf
- Nist SP800-161: https://doi.org/10.6028/NIST.SP.800-161
- NERC CIP 013-1
- NERC CIP 010-3
- NERC CIP 008-6
- FERC Order 850
- FERC Order 829
- FERC Order 848
- FERC Docket No. RD19-3-000
- NERC **2018 Compliance Monitoring and Enforcement Program Annual Report,** February 6, 2019
- Microsoft Supply Chain Paper: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVmcf
- NERC CIP-010-3 Guidance https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-010-3%20R1.6%20Software%20Integrity%20and%20Authenticity.pdf
- NERC CIP-013-1 Imp guidance: https://www.nerc.com/pa/comp/guidance/EROEndorsedImplementationGuidance/CIP-013-1-R1%20Implementation%20Guidance.pdf