

# Cybersecurity and Video Surveillance: **How to Protect Your IP Video Network**

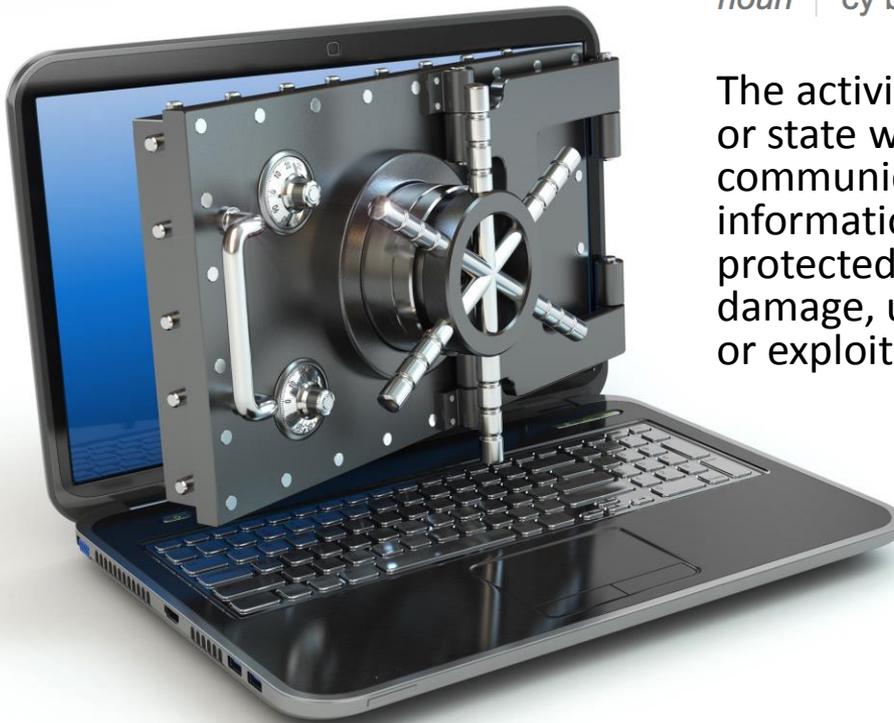
Presented by Joe Coe  
Hikvision USA Inc.

# What is cybersecurity?

## Definition:

*noun* | cy-ber-se-cu-ri-ty

The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.



Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National [Preparedness](#) Goal; White House Cyberspace Policy Review, May 2009



# Hon. Jeh Charles Johnson

Secretary of Homeland Security

# Who commits cyber crimes?

**Who?**

Potentially anyone who has access to the Internet.

**How?**

Viruses, malware, bots, or exploitation  
of software vulnerabilities.

# Viruses detected

**When?**

Impossible to predict.



**Where?**

“Cyberspace,” “The Internet,” “WWW”

**http://www**



**Why?**

A person wearing a grey hoodie and black gloves is shown in profile, focused on typing on a laptop keyboard. The background is a dark, solid red color. The person's face is partially visible, showing a beard and nose. The lighting is dramatic, highlighting the texture of the hoodie and the details of the gloves.

**HIKVISION**<sup>®</sup>

In the Video Surveillance world, cyber crimes are committed to cover up other crimes or to view video that should be private.

# Tips/Best Practices for Cybersecurity

# Tips/Best Practices *cont.*

Keep appliances current: update software and firmware regularly. As vendors find issues they work to create fix and patches that help prevent issues. Your due diligence is required.

# Tips/Best Practices *cont.*

Everyone should be assigned their own username and password.  
This ensures accountability.

## Tips/Best Practices *cont.*

Whenever possible, use a firewall appliance between your IT assets and the Internet. At the very least use NAT at your Internet gateway.

## Tips/Best Practices *cont.*

Use uncommon ports: “security through obscurity.” This creates an additional step when someone is trying to access your appliances.

# Tips/Best Practices *cont.*

When possible, put your network and IT assets behind locked doors to limit unnecessary access.

# Tips/Best Practices *cont.*

Make sure you are using password lock-out features for invalid login attempts and if possible, receive notifications of these attempts.

# Tips/Best Practices *cont.*

Design a plan of who to notify in the instance of your appliances being compromised (or simply if you suspect that they have).

# Tips/Best Practices *cont.*

If you suspect a vulnerability is due to a flaw with the manufacturer, notify the manufacturer so that they can test.

If an issue is found they can also work to fix it.

# Recommendations for Vendors

# Recommendations for Vendors *cont.*

Have your products routinely tested by third parties to identify any vulnerabilities before cyber criminals do.

# Recommendations for Vendors *cont.*

Provide clear information on your website and in company communications on how to change passwords and upgrade firmware.

- E.g.: Hikvision's online Security Center
  - <http://www.hikvision.com/en/us/securitycenter.asp>
- E.g.: Videos about changing passwords and upgrading firmware
  - <http://www.youtube.com/hikvisionusainc>

# Recommendations for Vendors *cont.*

Train your technical support team to respond appropriately to cyberattack.

**Always remember:** No one is immune, *simply lucky*.  
If someone wants to spend enough time and effort  
they can find a way to get onto any device that is  
attached to the Internet.

**Thank You!**



# NERC CIP Cyber Security Compliance Management Solution

August 19, 2016

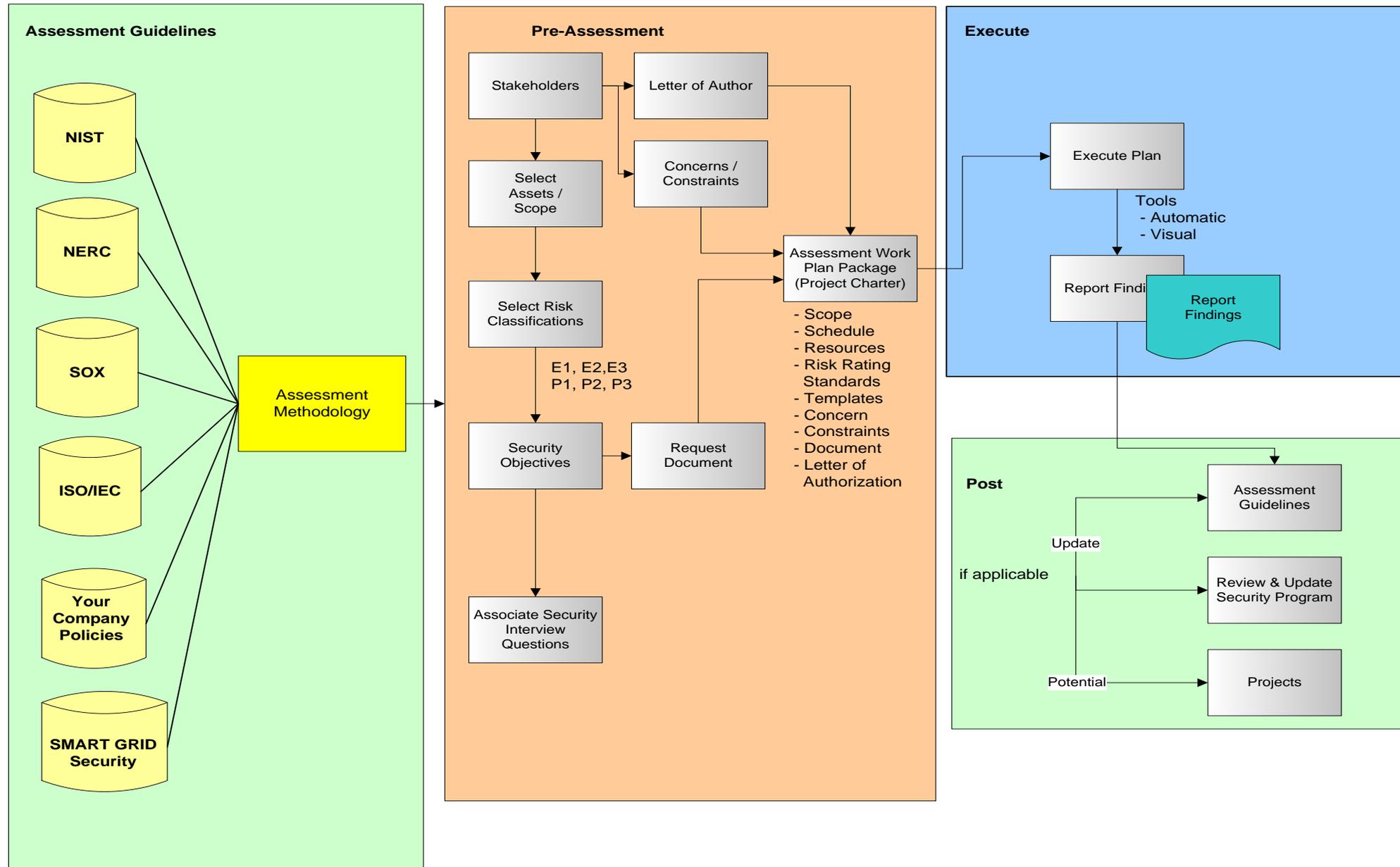
# Compliance Roadmap Development

- Categorize System
  - Impact Criteria of BES Cyber System? Low, Medium, High
  - Determine what Cyber Asset category or categories the product fits in
- Map to Requirements
  - Based directly on Impact and Cyber Asset category
- Assess State of Compliance
  - Review product documentation, development documentation, software and conduct interviews with developers
- Develop Guidance
  - Based on Requirement's Guidance and Technical Basis (GTB) and professional experience

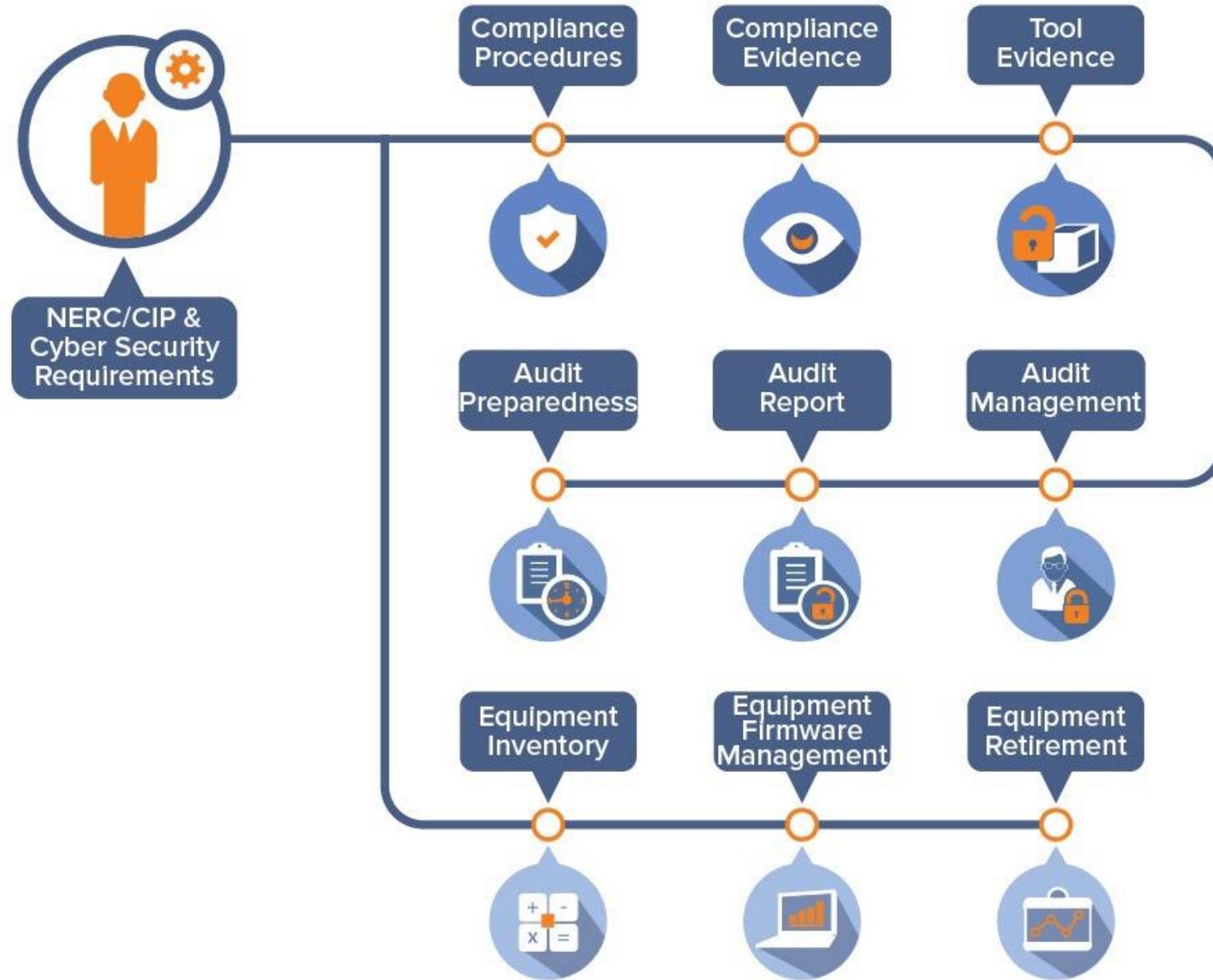
## Categorization

- Categorization of requirements affecting Product is based on the Facility where product is deployed (CIP-002-5.1) and the type of system the Product is a part of:
  - Impact Criteria: High, Medium, and (Low)
  - Cyber Asset Category: “EACMS”, “PACS”, “PCA”
- Since the Vendor does not know where their Product will be deployed, conservative assume High Impact criteria
- Cyber Asset Category based on actual product function and usage. In this case Product is a protected cyber asset “PCA”

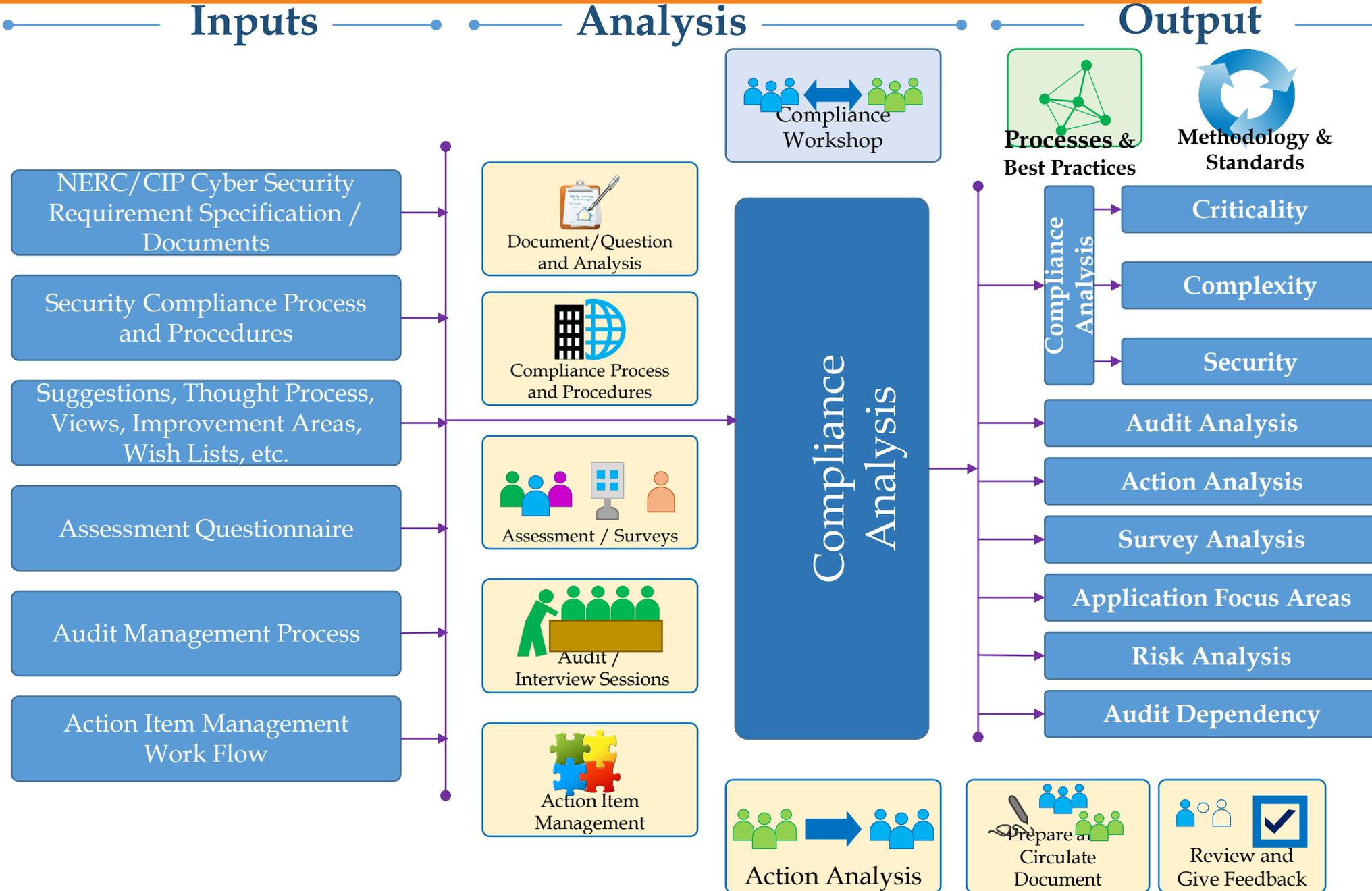
# Security Assessment Methodology



# NERC CIP Process Overview



# NERC CIP Process Overview



## Functionality Overview



## Security Baseline Assessment Checklist: Information Security Policy

Security Baseline Assessment Checklist		
Question(s)	Findings	Supporting Documentation
<b>Information security policy</b>		
Does an Information security policy exist which is approved by the management?		
Is the security policy published and communicated as appropriate to all employees?		
Does the policy state management commitment and set out the organizational approach to managing information security?	<b>Example</b>	
Does the Security policy have an owner who is responsible for its maintenance and review according to a defined review process?		
Does the review process ensure that a review takes place in response to any changes affecting the basis of the original policy?		
<b>Internal organization</b>		
Is there a management forum to ensure there is a clear direction and visible management support for security initiatives within the organization?		
Is specialist information security advice obtained where appropriate?		
Does management actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities?		

# Security Baseline Assessment Checklist: User Account Management

## Account Management Procedure Analysis

Audit Question(s)	Findings	Supporting Documentation
<b>User Account Management</b>		
Does the group designate and record individuals authorized to issue access to IT System resources and data?		
Is there a documented new user request process?		
Is a formal request form for new users utilized?		
Does the request contain name, organization (or name of contracting company and contract number if applicable), location, purpose for access, and access requirements?		
Are all requests reviewed by a manager to ensure that appropriate access is granted to new personnel?	<b>Example</b>	
Are procedures established for identifying, managing (adding and deleting users), recording, and monitoring who has access to sensitive IT System resources?		
How are passwords distributed to new users?		
Is a secure method utilized for the delivery of passwords?		
Is a password history enforced?		
Is a minimum password age configured?		
Is a maximum password age configured?		
Is a minimum password length established?		
Are passwords required to meet a minimum complexity?		
Is an account lockout threshold defined?		
Is an account lockout duration set?		
Is an account lockout reset configured after a set period of time?		
<b>Audit and Management Reviews</b>		
Is user access and privileges reviewed at a regularly interval for the appropriate level of access/continued need?		
Do reviews examine the levels of access of each individual, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up to date, and whether required training has been completed?		

# Security Baseline Assessment Checklist: Server Review

Server Review Checklist		
Audit Question(s)	Findings	Supporting Documentation
<b>BIOS</b>		
Is access to the BIOS restricted?		
Are servers be configured to boot off of floppies or CD-ROMS?		
<b>USB Devices</b>		
Do servers prevent the utilization of USB devices?		
<b>Deployment</b>	<b>Example</b>	
How are new servers deployed?		
How many different types of servers are there (DC, DNS, File, Print, Application)?		
Is a standard image utilized?		
How many images are there?		
What do the standard images include? (AV, Patching, Backup agents, drive mapping, etc)		
Has a standard build checklist been developed?		
Does this standard build checklist map to a standard?		
How often is the image/build reviewed and updated?		
<b>Users Rights</b>		
Are users that are granted administrative access to server documented?		
Are users granted access based upon least privilege?		
Are there shared users accounts?		
Has the local administrator account been renamed?		
<b>Data Backup</b>		
Is there a method to enable the backup process of server? (mapped drive, backup utility, etc)		
Is mission critical data stored on file servers with a formal data backup policy?		

# Security Baseline Assessment Checklist: Workstation Review

Workstation Review Checklist		
Audit Question(s)	Findings	Supporting Documentation
<b>BIOS</b>		
Is access to the BIOS restricted?		
Can workstations be configured to boot off of floppies or CD-ROMS?		
<b>USB Devices</b>		
Do local workstations prevent the utilization of USB devices?		
<b>Deployment</b>		
How are new desktops and laptops deployed?	<b>Example</b>	
Is a standard image utilized?		
How many images are there?		
What do the standard images include? (AV, Patching, Backup agents, drive mapping, etc)		
Has a a standard build checklist been developed?		
Does this standard build checklist map to a standard?		
How often is the image/build reviewed and updated?		
<b>Users Rights</b>		
What permissions are users granted on local workstations?		
Are users granted administrative rights to workstations?		
Are users that are granted administrative access to workstations documented?		
Are there shared users accounts?		
Has the local administrator account been renamed?		
<b>Data Backup</b>		
Is there a method to enable the backup process of workstations? (mapped drive, backup utility, etc)		
Is mission critical data stored on file servers with a formal data backup policy?		



## Audit Management

### Audit Management Module Configuration Step

- Modify template NERC CIP Requirements baseline based on your company specifics
- Modify baseline non-compliance causes based on your company standards



## Compliance Survey

### Audit Compliance Process Satisfaction Survey

- Modify baseline Audit Compliance Process Satisfaction Survey based on your company standards



## Standards Manual & Procedures

### NERC CIP Audit Requirements Manuals

- Modify baseline NERC CIP Manuals based on your company
- Modify baseline NERC CIP Procedures based on your company

# Audit Module: Work Steps

## Audit Management



## For Each Audit



## Print Audit Process



### Audit Management Module Configuration Step

Create your audit calendar by adding audit

Enter the name of the areas being audited (Transmission, IT, etc.)

Enter the date and the Audit System

Determine the users auditing (auditors) and the ones being audited (auditees)

Based on the procedures of the audited department, auditors create verification list with closed questions.

Auditors prints the verification list to carry out their audit

Or use the online version using a handheld device

## Audit Module: Work Steps

### Audit Management



- During or after the audit, Auditors fill in the answers of the verification list (conformed or not) with comments (evidences, references)
- Next, Auditors enter :
  - Strong points
  - Points to improve
  - Create Improvements opportunities
  - Non-Compliance

### Generate Audit Report

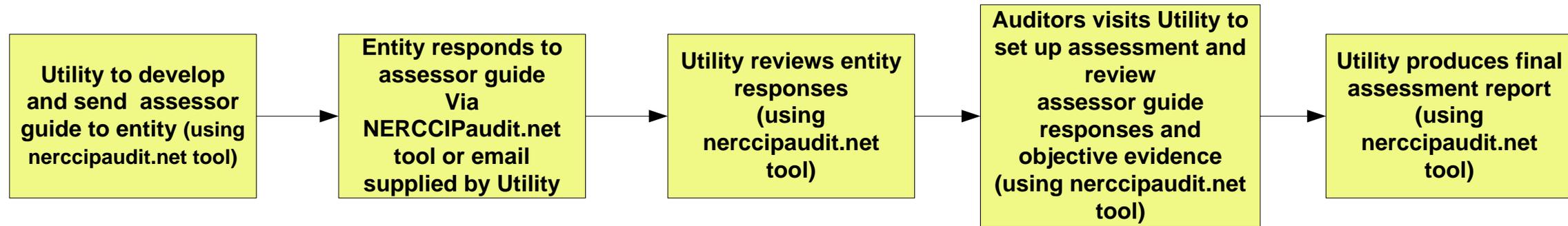


- Generate Audit Report

## Our Solution can be Used during the

### Pre-Audit Review and Assessment

The pre-audit review and assessment process proposed by NKSoft is shown in Figure below. It involves two phases. The first phase involves Utility responding to a questionnaire developed by NKSoft to request the identification of the objective evidence that will satisfy the requirements of the standards and the review of that information by the Utility's internal auditors. The second phase involves an on-site assessment by an Auditor assessment team to verify Utility's registration, verify the objective evidence identified by Utility in the first phase, and generate action items to resolve non-compliance issues or to improve objective evidence.



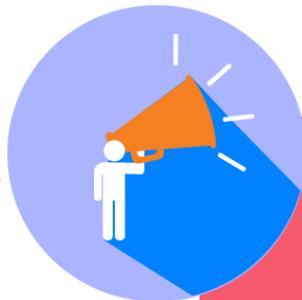
## Usage : Non-Compliance Management (NC)

### Non-Compliance Management



- Partner: Customer, supplier or company related to the NC
- Related to: Any reference pointing to the NC (order id, project id, task id, etc.)
- Responsible : User responsible for the NC
- Manager : User managing the department
- Origins : How the NC has been discovered
- Procedures : Against which procedure is the NC
- Description : Evidences, references to the standards
- Causes : Root causes
- Analysis : Result of the investigation
- opportunities
  - Non-Compliance

### Non-Compliance Action



- Actions and efficiencies : Actions and evidences that the actions were efficient, allowing Auditor to review actions and close NC

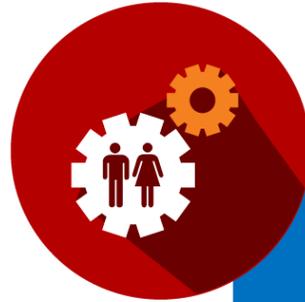


**Review Management**

- When creating review, enter :
  - Name:
  - Date : May 15th, 2016
  - Participants : the users involved in the review
  - Policy : Copy/Paste here your quality policy for re-evaluation
  - Changes affecting the system : List significant changes that needs to be planned and tracked by the top management
  - Survey answers : list of satisfaction survey answers filled in during April 2016
  - KPI : list of your KPI value for April 2016 (soon)
- Create one review line for each point to discuss among the inputs
- During the review, discuss each review line, note your decision and determine the output if any (action or nonconformity)
- In conclusion, determine the date and time of your next review

## Usage : Action for Non-Compliance Management (NC)

### Action Management



- When creating actions, Auditors enter :
  - Subject: What must be done
  - Deadline: Date by which the action must be completed
  - Responsible : User in charge of completing the action
  - Type : Immediate, corrective or preventive actions or improvement opportunity
  - Description : Details of the action

### Non-Compliance Action Review



- User in charge of the action enter notes and emails demonstrating the work in progress and close the action when completed.

Call or email us for a free demonstration

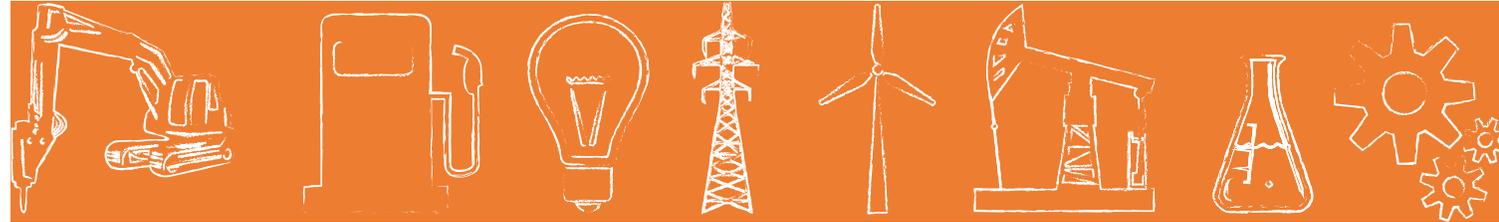
John Chowdhury

Phone: 214-213-6226

Email: [john@nksoft.com](mailto:john@nksoft.com)

# About NKSoft Solutions

## Project Development, Consulting & Research - Electric, Gas, Water Industry



NKSoft Utility Operations Services			NKSoft Smart Grid Program Services			Customer-Facing Smart Grid Services		
Grid Operations	Work, Field & Resource Mgmt..	Asset Management	MDM & Data Analytics	Network Communications And Cyber Security	System and Data Integration	Smart Customer Operations	CIS Initiatives	DSM & Energy Efficiency Implementations
Program Management, Smart Grid Strategy, Data Analytics, Change Management, Smart Managed Service (BPO)								



# Research and Recognition



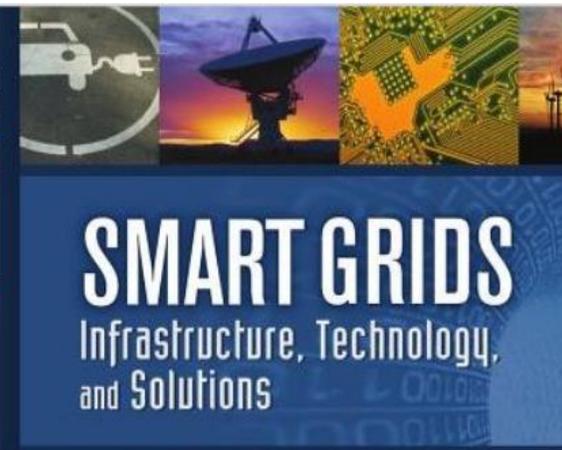
**Dallas Business Journal**  
CONGRATULATIONS TO  
*John Chowdhury*  
2ND YEAR IN A ROW  
FOR WINNING  
the Dallas Business Journal's  
TOP ENERGY



WE INVITE TO ATTEND  
THE NATIONAL RURAL ELECTRIC COOPERATIVE (NRECA)  
TECH ADVANTAGE SHOW  
IN NASHVILLE, TN  
ON TUESDAY, MARCH 4

JOHN CHOWDHURY & LUIS REYES,  
WILL BE DISCUSSING

DEVELOPING A  
TTT) NETWORK PLAN



**SMART GRIDS**  
Infrastructure, Technology,  
and Solutions




FOR WINNING  
the Dallas Business Journal's  
"TOP ENERGY"  
Join John at the party for  
"Dallas Petroleum Club" to  
Please Contact Dallas Business Journal



North American Policies and Technologies  
**ELECTRICITY Today**  
Transmission & Distribution  
FREE SUBSCRIPTION

Electric Cooperative, Inc. developed a  
the-Home network project plan to bring  
ess and economic prosperity as well as  
northern New Mexico.

the key components to the project plan  
berstand how to determine the right  
ossible master network integrator for

T&D Companies	T&D Products	Smart Grid	Electrical Substations	Smart Metering	Overhead T&D
---------------	--------------	------------	------------------------	----------------	--------------



**Cu** Canadian Copper & Brass Development Association  
Copper Alliance



**JOHN CHOWDHURY**  
Utility Practice Director,  
Fujitsu Network Communications, Inc.

Home > Smart Grid > Network Security

## Network Security

Protecting sensitive customer and utility data

BY JOHN CHOWDHURY, Fujitsu Network Communications, Inc.

Smart meters, and the advanced metering infrastructure (AMI) on which they depend, collect and transport vast amounts of data. While the data provides more precise energy billing, as well as valuable insight into energy demand and usage patterns, consumers expect that utilities will keep that data secure and that their privacy will be protected.

Security and privacy are prerequisites to increased AMI



## TECHNOLOGY SPOTLIGHT

### Security Safeguards + Customer Privacy = Smart Grid Success

The modern business world is awash in data, and utilities are certainly no exception. Smart grid architectures use sophisticated technologies to collect and transport vast amounts of data. While the proliferation of data provides valuable insight into energy demand and usage patterns, it comes with an expectation that utilities will

demand for greater smart grid security will only increase. Where traditional security logic says we should isolate our vulnerable operational control systems and customer data, smart grid causes us to "open up" access to our customer data, and our command and control systems to integrate and interconnect with other systems.

# Consulting Services

## Smarter Utility Consulting

We provide solutions and services to utility (Electric, Water, and Gas) to Energy Companies around the world.

### NKSoft Utility Operations Services



#### GRID OPERATIONS

SCADA  
DMS/OMS/EMS  
Smart Grid Communications  
Grid Operations  
Cyber Security  
Power Systems Engineering



Work and Asset Management  
Work Diagnostics  
Supervisor Enablement  
Mobile Workforce Management



Asset Analytics  
Asset Investment Planning and Management  
Multi-resolution Asset Data Exchange  
GIS

### NKSoft Smart Grid Program Services



#### MDM & DATA ANALYTICS

Meter Data Management  
Network Communications  
Data Integration



#### NETWORK COMMUNICATIONS AND CYBER SECURITY

Network Strategy  
Network Design, Build, Trials  
Operations  
Support Systems  
Security Solutions



#### SYSTEM AND DATA INTEGRATION

IT/OT Convergence  
Data Analytics  
Data Integration

### Customer-Facing Smart Grid Services



#### SMART CUSTOMER OPERATIONS

Web Interface  
Energy Efficiency  
Rate Analytics  
Customer Support



#### CIS INITIATIVES

CIS Updates  
SAP ISU  
Oracle CC&B  
Custom Interface  
Analytics Integration



#### DSM & ENERGY EFFICIENCY IMPLEMENTATIONS

DSM Setup  
Energy Efficiency Program Setup  
EE Analytics  
Reporting

# Integration

Program Management, Smart Grid Strategy, Data Analytics