

Disclosure: What's Mandatory and What's Common Sense

Terry Thompson
General Auditor
Santee Cooper

COMPLIANCE WEEK 2012

Disclosure: What's Mandatory and What's Common Sense

Background

As an electric utility, Santee Cooper is required to comply with North American Reliability Electric Corp. (NERC) reliability standards. These standards define the requirements for planning and operating the North American bulk power system and are designed to minimize disturbances in the power system and ensure electricity is provided in a consistent manner.

Disclosure: What's Mandatory and What's Common Sense

Background

All bulk power system owners, operators, and users must comply with approved NERC reliability standards.

Failure to comply with NERC reliability standards may result in monetary penalties and damage to the companies public image.

Disclosure: What's Mandatory and What's Common Sense

Common Disclosure Concerns

- Underreporting due to unrecognized violations
- Underreporting due to poor execution or fear
- Reporting concerns that are not violations

Disclosure: What's Mandatory and What's Common Sense

Criteria for Disclosure Decisions

Corporate Policies

1. If violation exists, ***always disclose!!***
2. If uncertain that a violation exists, engage Legal and appropriate corporate officers to verify, and to report if violation has been confirmed.

Disclosure: What's Mandatory and What's Common Sense

Criteria for Disclosure Decisions

Corporate Policies

3. If a violation does not exist, we may disclose the condition as a close call. For example, if our Energy Management System goes down, this condition triggers an event, but does not necessarily equate to a reportable incident. (Goal is to be transparent.)

Disclosure: What's Mandatory and What's Common Sense

Corporate Policies

4. All reportable items are reported to a manager at the officer level, executive management, and the Board of Directors.
5. All violations are reported expeditiously and tracked until violations have been resolved.

Disclosure: What's Mandatory and What's Common Sense

Internal Control Practices

- Internal training/awareness of regulatory requirements
- Corporate policies and procedures, including monitoring & oversight and escalation processes
- Internal reviews of operating systems to verify systems are developed or upgraded to meet operating requirements

Disclosure: What's Mandatory and What's Common Sense

Internal Control Practices

-Whistleblower hotline

-Liaison for regulators

1. Establish clear understanding of regulatory requirements and best practices.
2. Maintain awareness of future regulations and impacts.

Disclosure: What's Mandatory and What's Common Sense

Jay M. Cohen
Chief Compliance Officer
Assurant

COMPLIANCE WEEK 2012

Disclosure: Mandatory and Common Sense

The decision whether to self-report is...

- An increasingly common and critical part of your job
 - Fraught with peril and consequences
- Likely to be second-guessed – internally and externally
- Only possible at the end of a series of steps that you must plan for now, and execute well

Disclosure: Mandatory and Common Sense

These issues require advance attention, so you can make informed and defensible decisions

- Information: what do you know, when do you know it?
 - Investigation: how, by whom and how quickly?
 - Escalation: how high must you go?
- Response: whose help will you need to stop-and-fix?
- Analysis: what are the competing considerations and how will you weigh them?

Disclosure: Mandatory and Common Sense

- **Step 1 – Information: If, when and how will you know what has happened?**
 - Most information is reported to managers, not to your helpline. Will they tell you?
 - The more distant the office, the less likely the report
 - But you are responsible, whether you know or not!
 - Tools -
 - Mandatory reporting by managers – consequences for not
 - Leadership scorecard
 - Face time – overcome skepticism

Disclosure: Mandatory and Common Sense

- **Step 2 – Investigation: Are the resources in place ahead of time to assess and investigate?**

- Have you matched resources to categories of cases, evidence, investigation?

This matching requires an assessment of

- Internal capabilities and external resources
- Timeliness, cost, privilege, complexity, credibility

- **Tools**

- Investigative manual and response plan
- Training and practice
- On-call external experts

Disclosure: Mandatory and Common Sense

- **Step 3 – Escalation: Who do you tell inside the company and when?**
 - There are requirements: SOX 302 and 307
 - But what if internal self-reporting is NOT required?
 - Can it wait for your “regular” report, or do you need to call now? Report all or report some?
 - Outsiders expect the board to know more, not less
 - Tools
 - Work this out now with the Board and senior management
 - Investigative manual – general outline with flexibility

Disclosure: Mandatory and Common Sense

- **Step 4 – Response: Have you stopped and fixed the problem, whether or not you report?**
 - Do not ignore remediation while you are investigating
 - This is easier said than done. What will it take to:
 - Stop the problem
 - Fix what has already happened
 - Make changes going forward
 - Tools: individual discipline is only one factor
 - Assessment of the harm – who suffered and how much?
 - Understanding and commitment from the top
 - Money

Disclosure: Mandatory and Common Sense

- **Step 5 – Analysis: Do I understand all of the competing considerations and consequences?**
 - Nature and seriousness of the matter, isolated or not
 - Senior leadership knowledge and involvement
 - Have I done enough or too little to find out?
 - Whistleblowers: the 120-day clock is ticking
 - Regulations and external expectations, even if no “duty”
 - Race to the regulator versus rush to judgment
 - Collateral consequences
 - Risks and benefits of cooperation

Disclosure: Mandatory and Common Sense

- **Conclusion**

- Plan ahead
- Line up your resources
- Educate your leadership
- Recognize that this is not a linear process or a simple decision
- Take a deep breath
- Prepare to be second guessed
- Throughout this process, ask this question: Who are we?

Disclosure: What's Mandatory and What's Common Sense

Carl Lackstrom

*VP of Risk Management and Internal Audit
HMS, Inc.*



COMPLIANCE WEEK 2012

Disclosure: What's Mandatory and What's Common Sense

Disclosure Areas

- Investor relations/SEC filings
- HIPAA/HITECH compliance
 - PHI/PII breach
- Medicaid/Medicare regulations
- Other federal/state laws and regulations
 - Government contracting
 - False Claims Act
 - GLBA

Disclosure: What's Mandatory and What's Common Sense

Disclosure Challenges

- Internal notification and communication
 - What do we know?
 - When did we know it?
 - Employee awareness
 - Premature disclosure
 - Evaluation of facts
- Analysis of disclosure requirements
 - Rouge employee
 - Social media

Disclosure: What's Mandatory and What's Common Sense

Building Disclosure Capabilities

- Disclosure committee
 - Key executives
 - Individuals with sound judgment
 - GRC committee
- Legal, Compliance, Security, Quality, Risk & Audit
 - Incident/crisis management protocols
 - Who speaks for the company
- Timely, but vetted, disclosure communications

Disclosure: What's Mandatory and What's Common Sense

Building Disclosure Capabilities

-Training

- Annual employee compliance training
 - Management training
 - Executive/spokesperson training
- Ongoing security training and communications
 - Board communications and integration
 - Audit committee
 - Compliance (and risk) committee