TEXAS RE
Ensuring electric reliability for Texans

Ask Texas RE:

CIP-008-6 – Cyber Security Incidents: Incident Reporting and Incident Response Plan Testing

William Sanders

Cybersecurity Principal, Enforcement

Definitions

Cyber Security Incident

- A malicious act or suspicious event that:
  - For a high or medium impact BES Cyber System, compromises or attempts to compromise (1) an Electronic Security Perimeter, (2) a Physical Security Perimeter, or (3) an Electronic Access Control or Monitoring System; or
  - Disrupts or attempts to disrupt the operation of a BES Cyber System.

Reportable Cyber Security Incident

- A Cyber Security Incident that compromised or disrupted:
  - A BES Cyber System that performs one or more reliability tasks of a functional entity;
  - An Electronic Security Perimeter of a high or medium impact BES Cyber System; or
  - An Electronic Access Control or Monitoring System of a high or medium impact BES Cyber System.

Attempts to Compromise

- Defined by Responsible Entity

Requirements

CIP-008-6

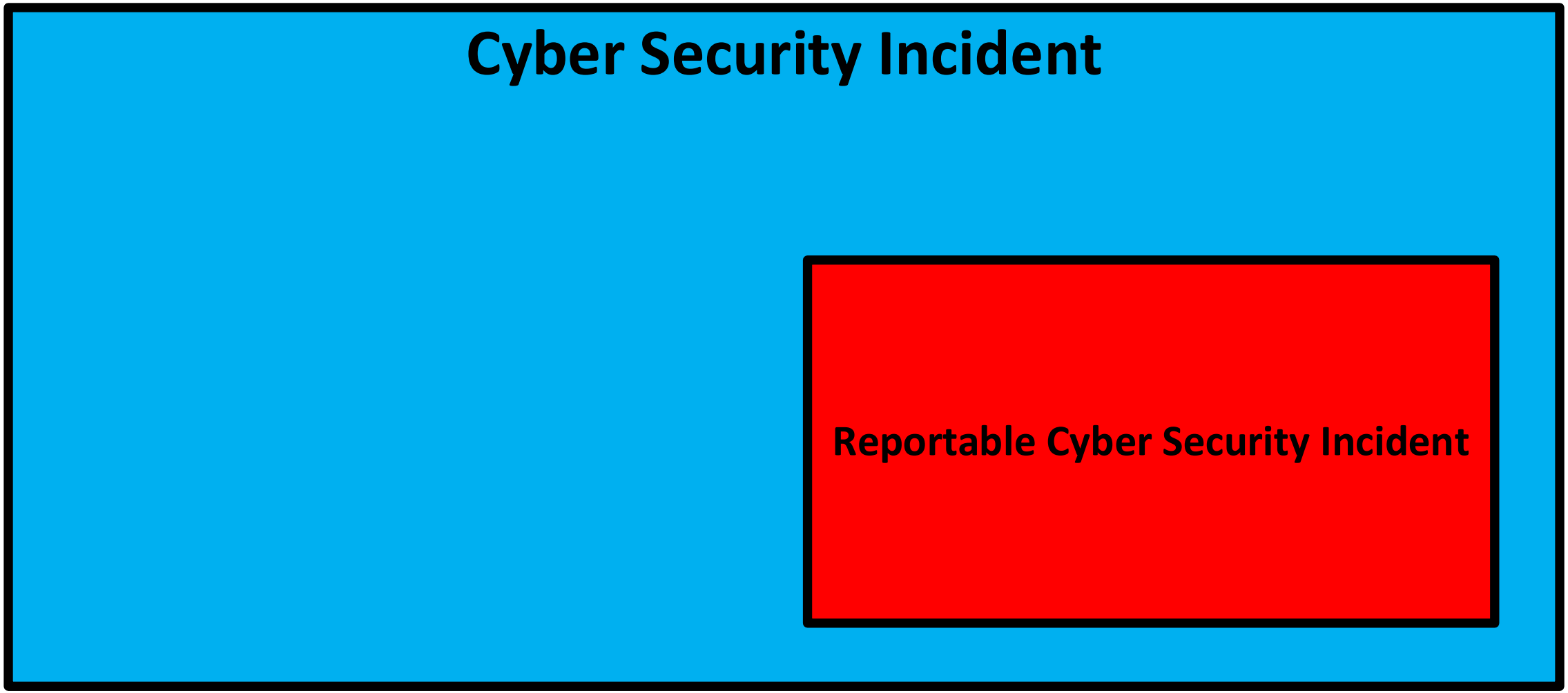
- R4. Each Responsible Entity shall notify the Electric Information Sharing and Analysis Center (E-ISAC) and, if subject to the jurisdiction of the United States, the United States National Cybersecurity and Communications Integration Center (NCCIC), or their successors, of a Reportable Cyber Security Incident and Cyber Security Incident that was an attempt to compromise, as determined by applying the criteria from Requirement R1, Part 1.2.1, a system identified in the "Applicable Systems" column, unless prohibited by law, in accordance with each of the applicable requirement parts in CIP-008-6 Table R4 – *Notifications and Reporting for Cyber Security Incidents. [Violation Risk Factor: Lower] [Time Horizons: Operations Assessments].*

Requirements

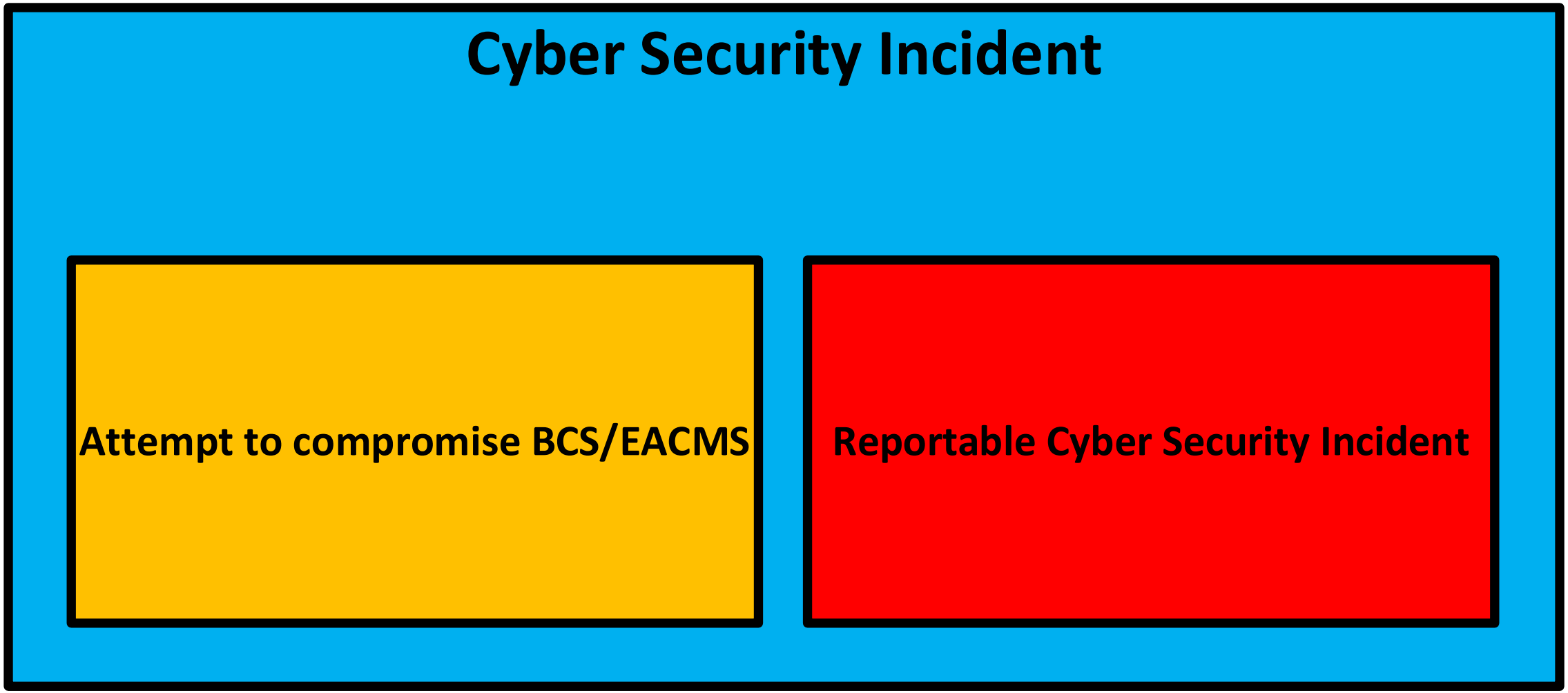
CIP-008-6 Table R2 – Cyber Security Incident Response Plan Implementation and Testing			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: • EACMS Medium Impact BES Cyber Systems and their associated: • EACMS	Test each Cyber Security Incident response plan(s) at least once every 15 calendar months: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise of a Reportable Cyber Security Incident; or • With an operational exercise of a Reportable Cyber Security Incident.	Examples of evidence may include, but are not limited to, dated evidence of a lessons-learned report that includes a summary of the test or a compilation of notes, logs, and communication resulting from the test. Types of exercises may include discussion or operations based exercises.

Interactions

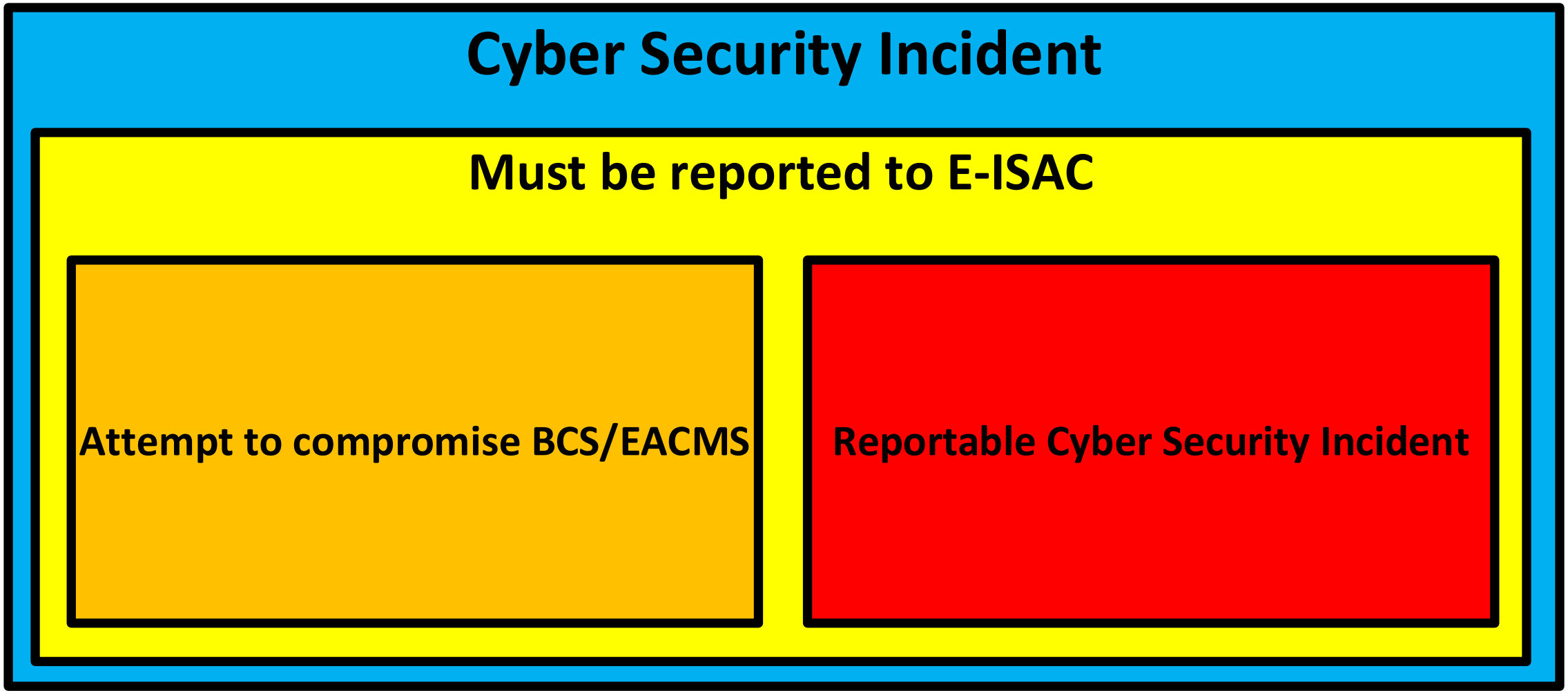
Interactions



Interactions



Interactions



Final

Per CIP-008-6 R4.2 attempts to compromise high impact BCS, medium impact BCS, or EACMS associated with high or medium impact BCS must be reported to the E-ISAC and applicable government authorities or their successors.

However, an attempt to compromise one or more high impact BCS, medium impact BCS, or EACMS associated with high or medium impact BCS does not meet the glossary definition of Reportable Cyber Security Incident.

An exercise of a Responsible Entity's Cyber Security Incident response plan using a scenario where there was an attempt to compromise, but no successful compromise, of a high impact BCS, medium impact BCS, or an EACMS associated with high or medium impact BCS will not satisfy periodic testing requirements outlined in CIP-008-6 R2.1. CIP-008-6 R2.1 requires that the Cyber Security Incident response plan be tested using a Reportable Cyber Security Incident.

TEXAS RE
Ensuring electric reliability for Texans