



TEXAS RE

Cybersecurity Awareness

Devin Ferris
Manager, CIP Compliance Monitoring

October 11, 2024

Security Awareness

CIP-004-7 R1

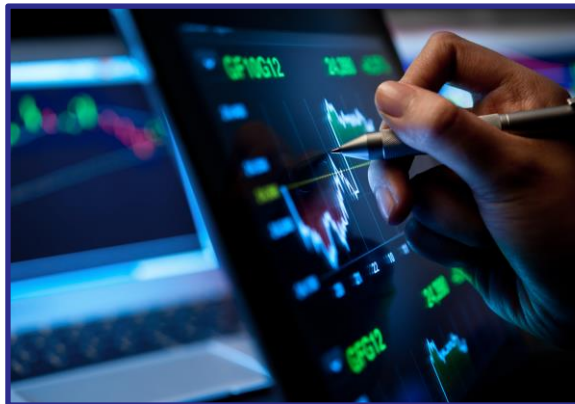
- Security awareness that, at least once each calendar quarter, reinforces cybersecurity practices (which may include associated physical security practices) for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems

CIP-003-8 R2, Section 1

- Cyber Security Awareness: Each Responsible Entity shall reinforce, at least once every 15 calendar months, cyber security practices (which may include associated physical security practices)



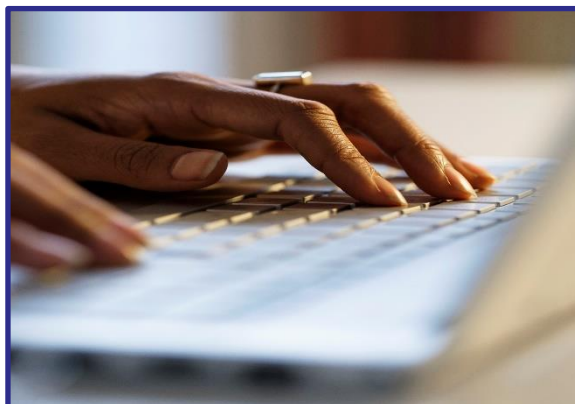
Security Awareness Examples



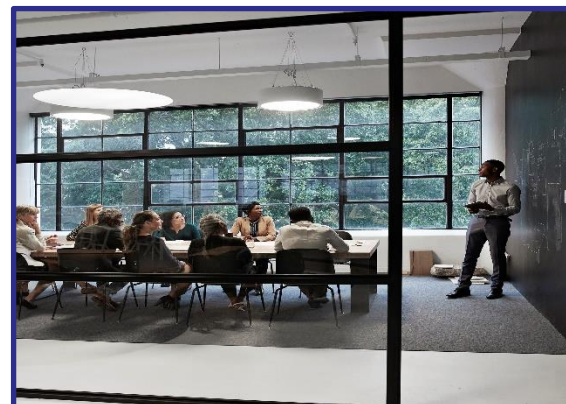
Measures “Examples”



Indirect Communications



Direct Communications



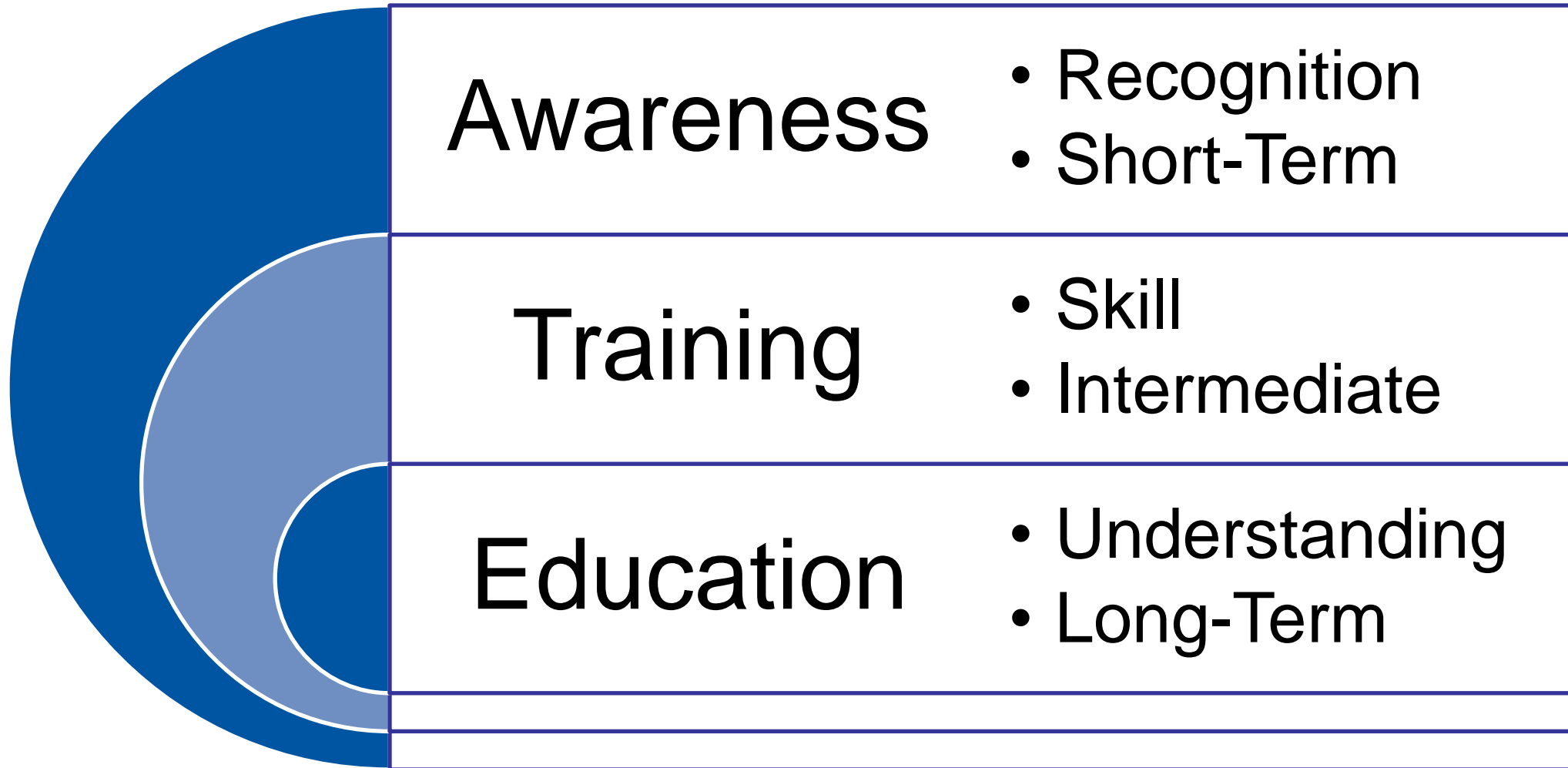
Management Support and Reinforcement

Cyber Security Training Program

CIP-004-7 Table R2 – Cyber Security Training Program			
Part	Applicable Systems	Requirements	Measures
2.1	<p>High Impact BES Cyber Systems and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS <p>Medium Impact BES Cyber Systems with External Routable Connectivity and their associated:</p> <ol style="list-style-type: none"> 1. EACMS; and 2. PACS 	<p>Training content on:</p> <ol style="list-style-type: none"> 2.1.1. Cyber security policies; 2.1.2. Physical access controls; 2.1.3. Electronic access controls; 2.1.4. The visitor control program; 2.1.5. Handling of BES Cyber System Information and its storage; 2.1.6. Identification of a Cyber Security Incident and initial notifications in accordance with the entity's incident response plan; 2.1.7. Recovery plans for BES Cyber Systems; 2.1.8. Response to Cyber Security Incidents; and 2.1.9. Cyber security risks associated with a BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets, including 	<p>Examples of evidence may include, but are not limited to, training material such as power point presentations, instructor notes, student notes, handouts, or other training materials.</p>



Cyber Security Training Program



Awareness and Training (AT) Control Family

AT-2 LITERACY TRAINING AND AWARENESS

Control:

- a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
 - 1. As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and
 - 2. When required by system changes or following [Assignment: organization-defined events];
- b. Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];
- c. Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
- d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.



The background of the slide features a blurred Texas state flag on the left and a close-up of a wind turbine's hub and blades on the right, all set against a clear blue sky.

Questions?



TEXAS RE

Ensuring electric reliability for Texans