From: **Dierking, Timothy**
Date: Thu, Mar 9, 2017 at 5:16 PM
Subject: NIST CSF Version 1.1 Feedback
To: "cyberframework@nist.gov" <cyberframework@nist.gov>

NIST CSF Version 1.1 Feedback:

- The Center for Internet Security (CIS) CSC is incorrectly referenced as “CCS CSC” in numerous places.
- PR.IP-1 has the incorrect reference to CCS CSC 10 (Data Recovery Capability), when it should reference CIS CSC 9 (Limitation and Control of Network Ports, Protocols, and Service) and CIS CSC 11 (Secure Configuration of Network Devices).
- PR.IP-2 should reference the CIS CSC 18 (Application Software Security)
- PR.AT-1 through 5 have the incorrect reference to CCS CSC 9 (Limitation and Control of Network Ports, Protocols, and Service), when they should reference CIS CSC 17 (Security Skills Assessment and Appropriate Training)
- PR.DS-1,2,5 have the incorrect reference to CCS CSC 17 (Security Skills Assessment and Appropriate Training), when they should reference CIS CSC 13 (Data Protection)
- PR.PT-2 should reference the CIS CSC 8 (Malware Defense)
- PR.PT-4 should reference the CIS CSC 8 (Malware Defense) and CIS CSC 12 (Boundary Defense)
- DE.AE-1 through 5 should reference the CIS CSC 6 (Maintenance, Monitoring, and Analysis of Audit Logs)
- DE.CM-3 should reference the CIS CSC 16 (Account Monitoring and Control)
- DE.CM -4 has the incorrect reference to CCS CSC 5 (Controlled Use of Administrative Privileges), when it should reference CIS CSC 4 (Continuous Vulnerability Assessment and Remediation) and CIS CSC 8 (Malware Defense)
- DE.CM-8 should reference CIS CSC 4 (Continuous Vulnerability Assessment and Remediation)
- DE.DP-4 should reference CIS CSC 12 (Boundary Defense)
- DE.AE-5 should reference CIS CSC 19 (Incident Response and Management)
- RS.RP-1 should reference CIS CSC 19 (Incident Response and Management)
- RS.CO-1 through 5 should reference CIS CSC 19 (Incident Response and Management)
- RS.AN-1 should reference the CIS CSC 6 (Maintenance, Monitoring, and Analysis of Audit Logs)
- RS.MI-1 through 3 should reference CIS CSC 4 (Continuous Vulnerability Assessment and Remediation)
- RC.RP -1 has the incorrect reference to CIS CSC 8 (Malware Defense), when it should reference CIS CSC 10 (Data Recovery Capability)
- There are numerous references to the CIS CSC, without a specific control number.

I would recommend mapping the CSF to the Microsoft Security Development Lifecycle and the Australian Signals Directorate (ASD) Strategies to Mitigate Cyber Security Incidents.

Best Regards,

Tim Dierking
Principal Systems Engineer
W: aclara.com A: 945 Hornet Drive, Hazelwood MO 63042