Role: Senior QA Evaluator (Contractor)
Context Overview:
While working as a Senior QA Evaluator, I identified and responded to a security compromise of a high-profile government official's Facebook page in another country. Although this was not labeled a GRC or cybersecurity role, the response aligned directly with core NIST 800-53, NIST 800-171, and CMMC frameworks — demonstrating real-world compliance instincts and technical mitigation under pressure.

Scenario: Government Official Page Compromise (International)

Event: A verified government page in Brazil showed signs of unauthorized access and possible malicious control.

Actions Taken:

- Flagged and escalated the incident to freeze the page.
- Conducted timeline tracing of account access changes.
- Identified potential compromise via malicious links or admin credential misuse.
- Recommended audit of all admin roles and their recent actions.
- Advised full password reset and implementation of MFA for all users.

Policy Framework & Control Mapping

Policy Area	Control Reference	Implementation Summary
Incident Response	NIST 800-53 / IR-4, IR-5	Identified and contained account compromise through immediate action and monitoring.
	NIST 800-171 / 3.6.1	Responded to a confirmed security incident involving unauthorized access.
Audit & Accountability	NIST 800-53 / AU-6	Reviewed admin access logs to determine timeline and responsible credentials.
	NIST 800-171 / 3.3.6	Used audit trails to support incident analysis.
Access Control	NIST 800-53 / AC-2(4), AC-6	Reviewed user privileges and ensured enforcement of least privilege among page admins.
Identification & Auth	NIST 800-53 / IA-2, IA-5	Recommended MFA and secure password reset to verify identity.
	NIST 800-171 / 3.5.3, 3.5.7	Strengthened access through multifactor authentication and password renewal.

Sample Policies (Plain Text)

Policy: Government Page Security Monitoring
Pages tied to verified public officials or high-profile entities must be continuously monitored for access anomalies and suspicious changes.

Policy: Freeze Protocol for Suspected Compromise
Upon detection of unauthorized access, immediate account freeze must be initiated to prevent further misuse. This action must be logged and escalated.

Policy: Audit Trail Review and Admin Accountability
All admin access logs must be reviewed to trace compromise origin. Any account showing anomalous activity must be deactivated until reverified.

Policy: Access Restoration and MFA Enforcement
After a confirmed breach, access may only be reinstated following full MFA setup and password reset for all authorized users.

Policy: International Data Escalation Protocol
Any incident involving foreign government data must be escalated through internal compliance channels, with consideration of international digital sovereignty and local regulations.

CMMC Considerations
Relevant CMMC practices demonstrated:

- **IR.L2-3.6.1:** Establish incident-handling capability.
- **AU.L2-3.3.6:** Correlate audit logs to detect and investigate incidents.
- **AC.L2-3.1.2:** Limit system access to the types of transactions and functions authorized.
- **IA.L2-3.5.3:** Use multifactor authentication.
- **IA.L2-3.5.7:** Enforce secure password policies.

Closing Note:
This incident shows that technical discernment and compliance instincts don’t require a title to be valid. Cybersecurity is often practiced through action — and this scenario proves the power of observation, policy thinking, and timely response.

#GRC #NIST #CMMC #CyberOps #IncidentResponse #MFA #AccessControl #MetaSecurity