From: Violeta Navarro

To: TACs and IT POCs

Date: May 18, 2023

Subject: Security Incident Reporting Reminder

Hi All,

This is just a reminder that agencies are required to report security incidents by completing the following form: http://www.wsp.wa.gov/_secured/access/docs/cjis_security_incident_report_form.pdf. See below CJIS Security Policy requirement for reference.

The last few months I have not received as many security incident reports as I have in the past. I am hoping that it is because agencies haven't experienced security incidents ☺

5.3.2 Management of Security Incidents

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

5.3.2.2 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

5.3.3 Incident Response Training

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

5.3.4 Incident Monitoring

The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

If you have any questions please let me know.

Thanks,

Violeta Navarro
Information Security Officer
ACCESS Section
Washington State Patrol
Office: 360-534-2161 VoIP: 16161
ACCESS Webpage