Consulting Report

2120 Incident Response Plan (IRP) Update

August 8, 2022

Cindy Rougeou, LASERS Executive Director
The LASERS Audit Committee

BACKGROUND

This was a planned engagement on the fiscal year end (FYE) 2021 Audit Plan. The fieldwork for this engagement was completed on May 24, 2022.

An IRP is a key component to minimizing the exposure of critical agency assets, i.e., LASERS data. Cybersecurity, while implemented and maintained by the Information Technology (IT) Division, is an agency responsibility. Cybersecurity-related attacks have become not only more numerous and diverse, but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all can be prevented. Therefore, an incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. To that end, an effective IRP provides the framework for handling incidents, particularly for analyzing incident-related data and determining the appropriate response to each incident.

IT developed an initial IRP version in 2019 and committed to an ongoing review and update of LASERS IRP process. As part of this process, IT initiated a project where they engaged CBI to assist with the review and update of the IRP.

SCOPE, OBJECTIVES, AND METHODOLOGY

The scope of this consulting project included the LASERS IRP.

The primary objective of this engagement was to review information related to the update of LASERS IRP.

Procedures used to complete this engagement included:
- Participating in meetings related to the IRP.
- Reviewing draft versions of the updated IRP.

This engagement was conducted in accordance with the Institute of Internal Auditors' <u>International Standards for the Professional Practice of Internal Auditing</u> and the policies and procedures of the Audit Services Division.

ENGAGEMENT SUMMARY

LASERS utilized the services of CBI, in a consultation role, to review and update LASERS IRP. Staff from IT and Audit Services participated in virtual meetings that took place in March 2021. The meetings helped IT identify possible revisions that should be made to LASERS IRP and provided guidance to develop supporting IRP documentation. LASERS approved the updated IRP in June 2022.

Examples of some key updates made to the initial IRP include the following:
- Outlining staff responsibilities.
- Redefining roles and responsibilities of staff members on LASERS incident response team.
- Defining incident identification and classification.
- Establishing a flow of events, escalation, and communications needed based on how an event is classified.
- Outlining requirements for collecting evidence.
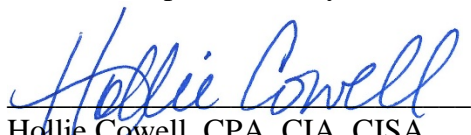- Adding additional contact information for various staff, vendors, and external reporting agencies.

According to IT, short-term plans for further IRP development include:
- Distributing the IRP to all LASERS staff and including it on the Intranet for reference.
- Educating the LASERS staff on the IRP and their responsibilities.
- Working with the Incident Response Team to collectively establish future improvements.

The Audit Services Division's involvement in IRP development was limited to the areas outlined in the Scope, Objectives, and Methodology section of this report. There were no reportable issues identified during this project.

FOLLOW-UP

No follow-up is necessary.

Hollie Cowell, CPA, CIA, CISA
Auditor

Ryan Babin, CPA, CIA, CISA
Audit Services Director

Cc: Trey Boudreaux
      Travis McIlwain
      Tina Grant
      Johnathon Sprouse
      Eric Schoonmaker
      Charles McBride