

State of Maine
Office of Information Technology
Information Security Office

Cyber Reliance Initiative Security Project: Phase 1
Cybersecurity

By: Nathan Willigar

July 2018 - December 2018

Phase 1

1.0 OVERVIEW

- 1.1 Historical assessments of the State of Maine information security posture continually found areas of unacceptable risk to the data and systems entrusted to the government. A significant project was undertaken to harden the cybersecurity infrastructure against possible threats to the network.
- 1.2 The State of Maine Cyber Reliance Initiative Security Project (CRISP) consists the employment of numerous technologies and techniques in select areas. The numerous interdependencies of the technologies employed speaks to the complexity of this undertaking.
- 1.3 The challenges faced by the Office of Information Technology was further compounded by the fact that the cyber infrastructure is vast in both quantity and diversity. The level of success achieved, despite the complex nature of the project, is worthy of commendation.

2.0 PROJECT AREAS – PHASE 1

- 1.4 The document attached outlines only some of the initiatives that were implemented/planned to be implemented within the past year. Our Government and services have never been stronger with the partnership of all areas within the Office of Information Technology and all our agencies focused on one goal of securing operations.
- 1.5 The following broad areas have been improved as a part of the project to address the numerous deficiencies in the State of Maine's ability to prevent and appropriately respond to cyber incidents:
 - 1.5.1 Defense in Depth – Comprised of enhancements from end-point managed services to the upgrade enterprise firewalls.
 - 1.5.2 Mobile Devices Security – Appreciating the network extends beyond our firewalls, efforts included secure remote access, mobile malware protection, and network connect to pulse secure client.
 - 1.5.3 Security Processes – Included improvements in election security, incident handling, strategic planning and security governance.
 - 1.5.4 Access Control – Developments in active directory user password aging, eliminating unapproved Virtual Private Networks (VPN) Software
 - 1.5.5 CIA of Data – Leveraging personal OneDrive storage and email data loss protection/prevention are but two components of how OIT improved data loss prevention and security.

3.0 CONCEPT

3.1 The State of Maine established a multiple year Cyber Reliance Initiative Security Project (CRISP) to tighten the cyber security for the Executive Branch of the State of Maine.

1.5.6 This is a multiple year project with a number of phases to address cybersecurity with the State of Maine.

1.5.7 This project is associated to both agile and waterfall approach based on funding and security initiatives.

1.5.8 This project is multiple million-dollar project with implementing new technologies and adding/repurposing staffing.

1.5.9 The Office of Information Technology in partnership with agencies are in the processing of forming the Information Security Governance Committee to assess and prioritize the initiatives over the multiple year project.

1.5.9.1 As part of the communications of the project, the Information Security Governance Committee will meet quarterly to review status reports.

1.5.9.2 Monthly reports are being provided to OIT Senior Management and Commissioner's Office.

4.0 SIGNIFICANCE

1.6 Key Point: The project will strengthen the State of Maine by tighten the protection of the agency data and operations by implementing security controls.

1.6.1 CRISP will strengthen compliance efforts with federal entities to prevent the lose critical sharing arrangements.

1.6.2 14 departments and 40 agencies will have tighter security to protect State of Maine citizens' data.

1.6.3 CRISP will highlight the importance of increasing the funding of cybersecurity into agency budgets to ensure adequate oversight and security are implemented.

5.0 IMPACT

5.1 The project will strengthen the protection of the State of Maine to ensure mission critical functions are operational to provide the services to the citizens and protect their data.

5.1.1 Historically, the State of Maine infrastructure and the view of cybersecurity has been weak and not priority. Since establishing CRISP, the Office of Information Technology culture has shifted to embrace the importance of baking security into operations.

5.1.2 In the past few years with all the reported cyber disruptions and data breaches from companies and other states, the State of Maine can't afford not to investment in strengthening our security posture. The cost of breach and the lack of trust by the citizens would sufficiently impact the services provided by the State of Maine.