Status Update: Cook County Information Security

SENSITIVE AND INFORMATION SECURITY RELATED

September 2021

Purpose

The Chief Information Security Officer's (CISO's) semi – annual report shall detail:

- The status of all Agencies' adoption and compliance with the Information Security Framework (ISF); and
- A summary of all advice and recommendations of each Agency regarding their unique considerations.

Addressed Multiple Cyber Threats – Aug '20 to Jan '21

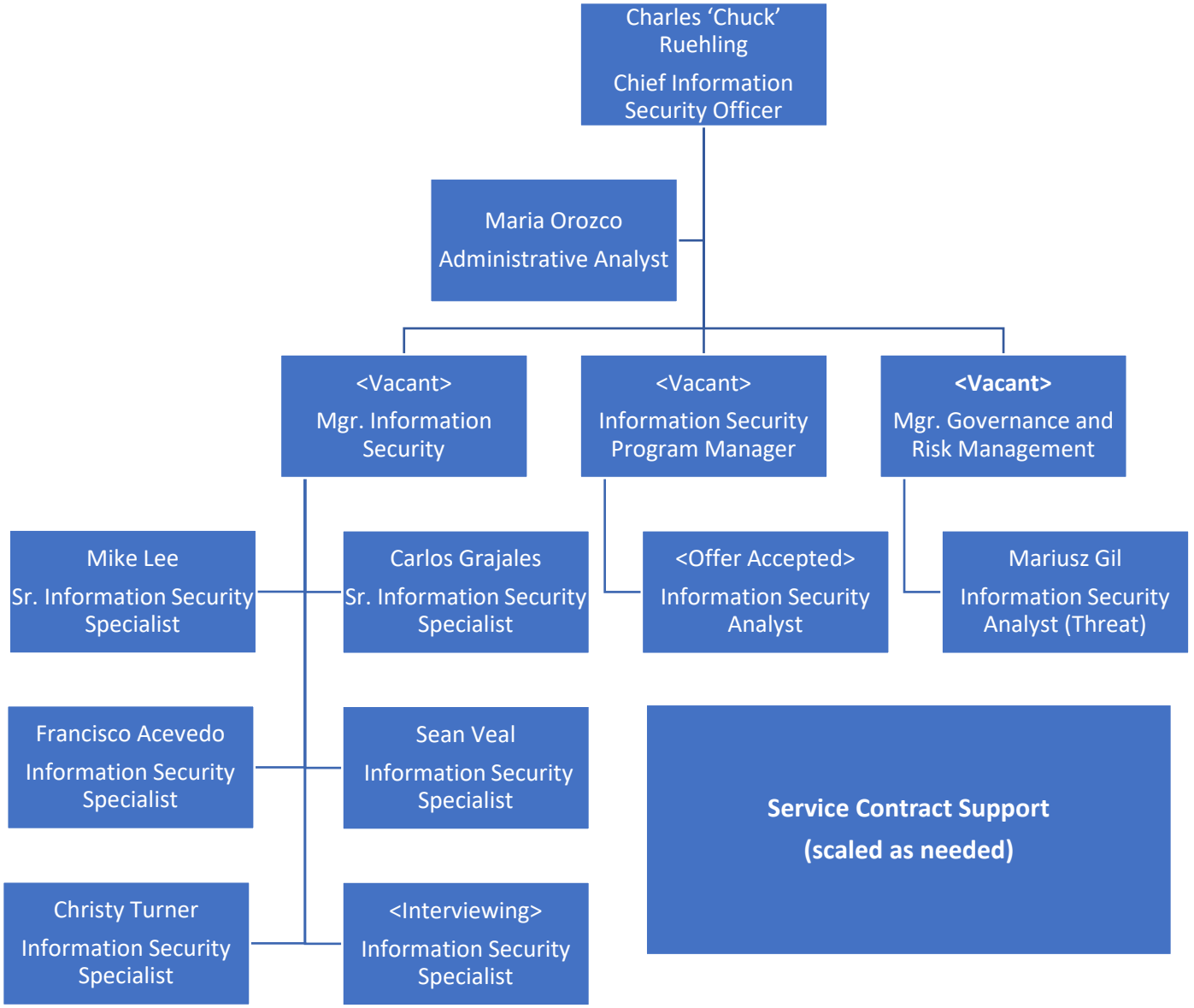
Eternal Blue Ransomware	EternalRomance Ransomware	Eternal Tools	WannaCry (leveraged EternalBlue and EternalRomance ransomware)	Bad Rabbit Ransomware
Petya/NotPetya Ransomware	Virut Malware	Kraken Malware	FaceAV Exploit Kit	Adobe Acrobat Memory Corruption Vulnerability (CVE-2017-3122)
Adobe Acrobat Professional security bypass vulnerability (CVE-2016-1041)	Adobe Acrobat Reader Memory Corruption Remote Code Execution (CVE-2017-11238)	Adobe Acrobat Reader Memory Corruption Vulnerability (CVE-2017-11240)	Adobe Acrobat Reader Open Type Font File Parsing Vulnerability	Adobe Acrobat Reader stack buffer overflow vulnerability (CVE-2017-2948)
Adobe Acrobat Reader Stack Buffer Overflow Vulnerability Denial of Service	Adobe Acrobat Reader Buffer Overflow Vulnerability (CVE-2017-3049)	Adobe Acrobat Reader Type Confusion Remote Code Execution (CVE-2017-11221)	Adobe Acrobat Reader Use After Free Vulnerability (CVE-2016-1089)	Adobe Acrobat Type Confusion Vulnerability (CVE-2017-16406)
Adobe Acrobat Use After Free Vulnerability(CVE-2016-0932)	Cisco Syslog DOS attacks	Adobe Reader – Too many to name individually	Adobe Reader– Too many to name individually	Adobe Shockwave Player – Too many to name individually

Total Events: 88,322,200,886

Security Events: 963,187,038

Incidents (Tickets): 1,226

Information Security Office Organizational Chart



Information Security Office (ISO) Major Events

February 2021 – July 2021

Recruited, Interviewed and Hired One ISO Team Member – Information Security Analyst

→

February 2021

Consolidated (Local) Primary Election Support to the Cook County Clerk's Office

→

March 2021

Completed MSSP RFP Proposal Review and received CIO Concurrence

↓

April 2021

Consolidated (Local) Election Support to the Cook County Clerk's Office

→

May 2021

Sean G. Veal Graduated from the IMPACT Leadership Development Program Class of 2021

→

June 2021

Urban Area Working Group (UAWG) Approves 1% decrease in ISO UASI 2021 Grant Funding

↓

July 2021

Managed Security Service Provider (MSSP) Contract Expires and is Replaced by new MSSP provider

→

Team Building

Recruiting and Retention

Gap Analysis / Prioritize Resources

Agency Support

- Completed All Drafts of the Information Security Framework Policies Based on the NIST Risk Management Framework (RMF) – in Total 20 Policies
- Completed Request for Proposal (RFP) Review Process for expiring Managed Security Service Provider (MSSP) contract and Awarded new Four (4) Year Contract
- Continued to Mature the Information Technology (IT) Concurrence Process, Integrating a Supply Chain Risk Management Step for IT Vendors not Currently in use.
- Working with Several Agencies to Integrate Two-Factor Authentication (2FA) into their IT Environments

2021 Projects / Events

SYSTEM SECURITY PLAN DEVELOPMENT IAW NIST 800-53 CONTROL SET

- In 2021, the Information Security Office (ISO) will develop a System Security Plan (SSP) in accordance with the NIST RMF set of Policies in preparation for a comprehensive Security Assessment of all ISO Security Controls.

INFRASTRUCTURE REFRESH OF THE SECURITY TOOL STACK

- Through the remainder of 2021, the ISO will continue the refresh of the security tool stack that is at end of life for vendor support while evaluating capabilities.

PREPARE FOR INFORMATION SECURITY OFFICE GRANT BUDGET SHORTFALL

- Build the request and justification for some ISO provided security capabilities moving to a fixed charges model as early as Cook County FY 2023.

INFORMATION SECURITY OFFICE STAFFING

- Recruit and retain motivated cybersecurity talent that is technically proficient, team-oriented and service-minded. Leverage contract resources to enhance capabilities where appropriate.

Cyber Security Challenges

Information security is a continuous process that requires due diligence, expertise and collaboration from all agencies to ensure that Cook County is adequately prepared for cyber security threats.

A modern cybersecurity program must have Board and Executive level visibility, funding and support.

Questions