BOARD OF HOMELAND SECURITY

WEDNESDAY, DECEMBER 2, 2020
10:00 TO 11:30 AM
MEETING VIA WEBEX/CONFERENCE CALL

BOARD MEETING MINUTES

Board Members Present:
James Stallings, Vice Chairperson
Vic Reynolds
Col. Chris Wright
MG Thomas Carden
Mark Williams
Gary Black
Calvin Rhodes
Kyle Sapp
Bill Cowsert
Alan Powell

Representatives Present:
Larry Barnes
Cristina Correia
Ashley Harris

Board Members Absent:
Chris Carr
Kathleen Toomey
Richard Woods
Russell McMurry

The Board of Homeland Security held the board meeting on December 2, 2020 via conference call. A List of Attendees, the Agenda, and the Board Presentation are attached hereto and made official parts of these minutes as Attachments #1, #2, and #3. Director James Stallings called the meeting to order at 10:00 AM.

All board members are present except Attorney General Chris Carr with the Georgia Department of Law, Commissioner Kathleen Toomey with the Georgia Department of Public Health, Superintendent Richard Woods with the Georgia Department of Education, and Russell McMurry with the Georgia Department of Transportation.

Vice Chairperson James Stallings welcomed everyone to the call.

Roll Call

Approval of the Minutes:
Vice Chairperson James Stallings postponed the approval of the February 5, 2020 meeting minutes since a quorum was not present.

Vice Chairperson James Stallings postponed the approval of the June 3, 2020 meeting minutes since a quorum was not present.

Old Business:
Vice Chairperson James Stallings asked the Board for discussion on any old business.

Joey Greene provided a legal update for the members of the Board. Philip Peacock with Georgia Power has resigned from the Board. There are two vacancies on the Board of Homeland Security and the Governor's Office will make those appointments. There will be elections at the next Board Meeting in January for Vice Chairperson and Secretary.

New Business:
Vice Chairperson James Stallings opened the floor for discussion on any new business.

a) Cyber Security

David Allen with the Georgia Technology Authority presented on Cyber Security and an overview of the Office of Information Security (OIS).

See Attachment #3 for full presentation

b) Overview of Homeland Security Grant Funding

Harlan Proveaux provided a brief overview of the 2020 Homeland Security Grant Funding. Currently, GEMA/HS is meeting with the subrecipients and awarding the grants. There are some new requirements this year from the federal government. The grant funding is split 80% to local governments and 20% to the State. The funding must go towards the four national priorities of cybersecurity, soft targets, information sharing and cooperation, and emerging threats.

Adjournment:
There being no further business to be brought before the Board, Vice Chairperson James Stallings adjourned the meeting at 10:55 AM.

Official Attachments:

1. List of Attendees
2. Agenda
3. Board Presentation

BOARD OF HOMELAND SECURITY

WEDNESDAY, DECEMBER 2, 2020
10:00 TO 11:30 AM
MEETING VIA WEBEX/CONFERENCE CALL

BOARD MEETING ATTENDEES

Board Members:
James Stallings, Vice Chairperson
Vic Reynolds
Col. Chris Wright
MG Thomas Carden
Mark Williams
Gary Black
Calvin Rhodes
Kyle Sapp
Bill Cowsert
Alan Powell

Representatives:
Larry Barnes
Cristina Correia
Ashley Harris

Others Attending:
Anna Braue
Joey Greene
Harlan Proveaux
Ashley Seay
Mike Smith

Board of Homeland Security Meeting

AGENDA

December 2, 2020
10:00 - 11:30 A.M.
Meeting via WebEx/Conference Call

gema.webex.com OR call 1-855-282-6330
Meeting Number: 178 298 6528
Password: HS120220

Agenda Topic	**Speaker**
Call to Order	James C. Stallings, Vice Chairperson GEMA/HS
Roll Call	
Approval of Minutes from February 5, 2020	
Approval of Minutes from June 3, 2020	
Old Business	James C. Stallings, Vice Chairperson GEMA/HS
New Business	
a) Cyber Security	David Allen, CISO GTA
b) Overview of Homeland Security Grant Funding	Harlan Proveaux, Deputy Director GEMA/HS
Adjournment	

GEORGIA TECHNOLOGY AUTHORITY

Board of Homeland Security

Office of Information Security (OIS) Overview

David Allen - CISO

OUR VISION

A transparent, integrated enterprise where technology decisions are made with the citizen in mind

—

OUR MISSION

To provide technology leadership to the state of Georgia for sound IT enterprise management

December 2nd, 2020

Agenda

GTA OIS Mission and Strategy

Cyber Trends

Board Mission Area Applicability

Prevention and Protection

Response and Recovery

Recommendations

Questions / Discussion

GTA Mission & Strategic Goals

GTA's mission: To provide technology leadership to the state of Georgia for sound IT enterprise management

GTA IT Strategic Goal 1: Build a culture of information security awareness, preparedness and resilience, and mature the State of Georgia information security program

OIS Strategic Priorities

1. Enhance security on state networks
2. Develop a cyber-ready workforce
3. Build enduring partnerships

Top Four Drivers of Cybersecurity Complexity

1-Sophistication and **sheer range of cyber threats** continue to evolve

3- Regulatory complexity is growing

The cyber risk landscape continues to rapidly evolve.

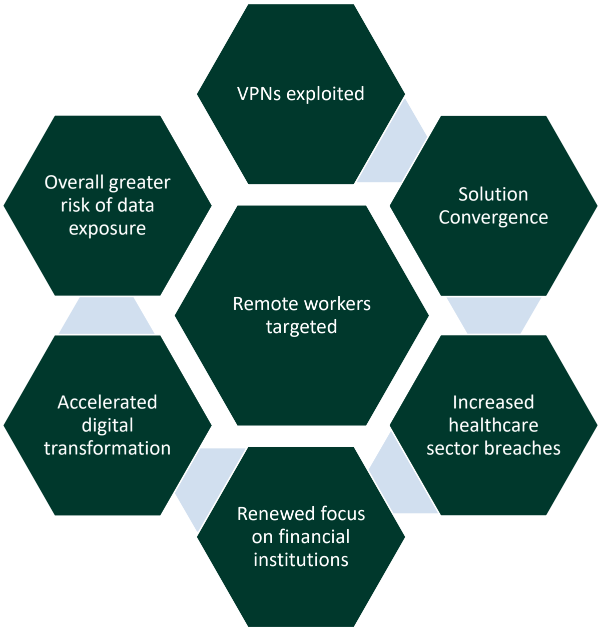
The CISO's job of safeguarding state's information assets is getting more challenging.

2- Complex and **mostly federated state government environments** pose governing challenges

4- Difficulty with resolving competing fiscal requirements

Top Cybersecurity Trends for 2021

- Cybercriminals took advantage of the sudden move to remote work
- Exploit of unpatched VPNs and other remote access technology
- Solution convergence due to reduced IT spending
- Financial pressures on the healthcare industry further decrease security funding
- Increased attacks toward institutions maintaining financial data
- Digital transformation a ‘silver lining’
- Data / Identities = “currency”



VPNs exploited

Overall greater risk of data exposure

Solution Convergence

Remote workers targeted

Accelerated digital transformation

Increased healthcare sector breaches

Renewed focus on financial institutions

This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

BoHS Mission Areas Applicable to OIS

Prevention – Actions to avoid an incident or to intervene or stop an incident from occurring

Protection – Actions to reduce the vulnerability of critical infrastructure or key resources

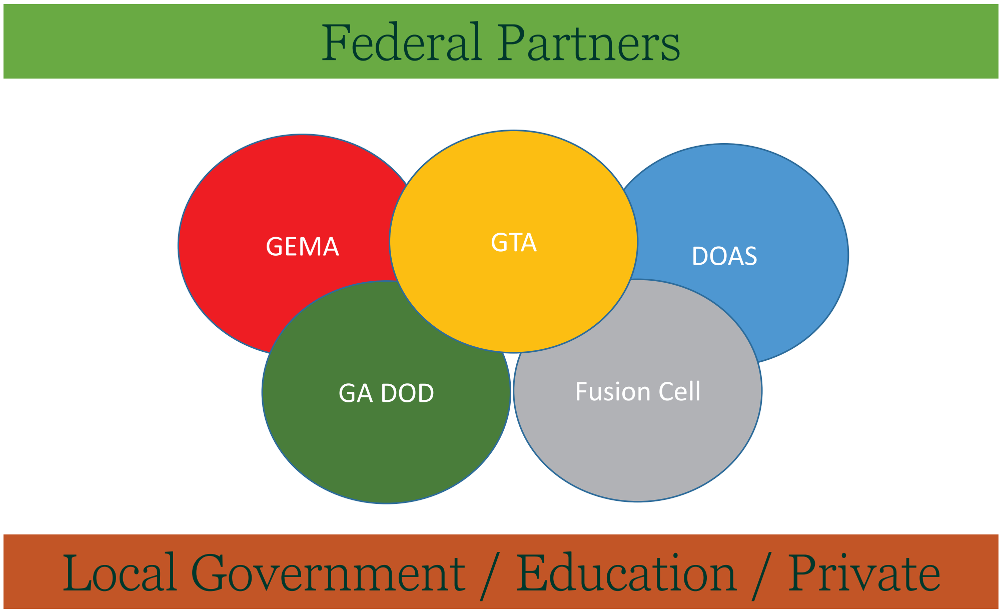
Response – Activities that address the short-term, direct effects of an incident

Recovery – Activities that include the development, coordination, and execution of infrastructure restoration plans

This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

- Federal Partners: FBI, DHS, CISA, and DOD provide free resources for prevention and incident response.
- GEMA: Controls overall emergency response, to include Cyber severity 1 incidents.
- GTA OIS: Responsible for initial incident response triage within the executive branch and outside the executive branch as delegated by GEMA. Maintains security contracts available for state/local use.
- DOAS: Maintains executive branch cyber insurance policy.
- Fusion Cell: OIS maintains personnel in the fusion center and is partnered with the Cyber Crimes Task Force.
- GA DOD: Maintains resources via the Cyber Protection Team for response to SEV 1 incidents and overall training support.

GA Government Cyber Ecosystem



This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

Prevention and Protection

Prevention/Protection: OIS Outreach

- Monthly Information Security Officer meetings open to all branches, state and local
- OIS actively shares threat intelligence to all state and local partners
- Cyber awareness presentations to multiple state and local government agencies in 2020
- Cyber Workforce Academy training in cooperation with the Georgia Cyber Center (GCC)
- Annual Cyber Dawg exercise at GCC in cooperation with GA DOD
- On-demand tabletop facilitation for state agencies

Cyber Awareness Training 2020

New Hire Training Schedule

- 90-day duration
  - Training modules - ***Introduction to Phishing; Protection Against Ransomware***

Ongoing Scheduled Training: 2020

- **Q1:** Training modules - ***Security Essentials; Social Engineering***
- **Q2:** Phishing campaign + additional training – Retake New Hire Training Assessment that will drive additional training modules
- **Q3:** Training modules - ***Avoiding Dangerous Attachments; Data Protection & Destruction***
- **Q4:** Phishing campaign + additional training – Retake New Hire Training Assessment that will drive additional training modules
  - Cybersecurity Awareness Month Activities

Assessments and Scanning

- **External vulnerability detection and scanning**:
  - MS-ISAC monthly web profiler (in-production)
  - BitSight Cyber Risk Rating Service (roll-out ongoing)
  - Vulnerability Disclosure Program (pilot completed September, full production June 2021)
  - Tenable Vulnerability Management System (GETS+)

- **Assessment Sequence of Events (6-8-week engagement)**
  - Pre-scan and document collection
  - Documentation analysis and interviews
  - 2nd vulnerability scan and final report development
  - Executive summary and findings delivered

This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

Response and Recovery

REDACTED

This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

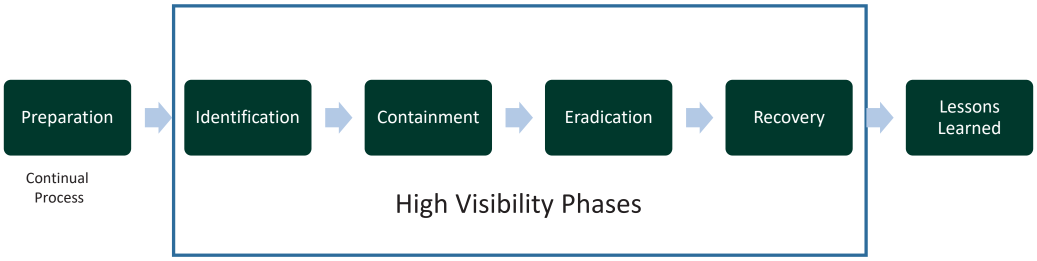
REDACTED

This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

REDACTED

This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

Response/Recovery: Incident Handling Methodology

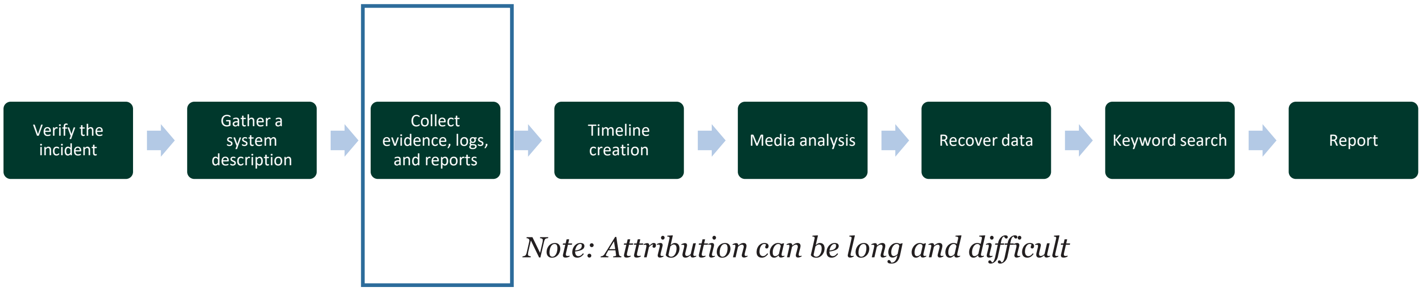


Note: Completion intervals for each phase vary widely

Source: The SANS Institute

This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

Response/Recovery: Forensics Methodology



Verify the incident

Gather a system description

Collect evidence, logs, and reports

Timeline creation

Media analysis

Recover data

Keyword search

Report

Note: Attribution can be long and difficult

Source: The SANS Institute

This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

REDACTED

This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

REDACTED

This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

Lessons Learned - Ransomware

1. Get vendor partners involved early
2. Ensure proper licensing on all products prior to recovery
3. Use as an opportunity to evaluate candidates for cloud transition
4. IT shops need a designated security rep that is properly trained and credentialed
5. An adequate backup solution saves significant time and $$
6. Insurance is not a 100% solution

This document is protected from disclosure by O.C.G.A. 50-18-72(a)(25)(A)(i) (2013) and should be kept confidential to protect the interests of the public.

Recommended Next Steps – Homeland Security

1. Continue development / communication of incident reporting process
2. Continue evolving and integrating threat intelligence processes
3. Increase cyber education / training to the local level
4. Continue inter-agency cooperation for cyber events and exercises
5. Encourage cyber incident response plan development at the local level

Questions/ Open Discussion