BOARD OF HOMELAND SECURITY

WEDNESDAY, JUNE 1, 2022
1:30 TO 3:00 PM
GEMA/HS HEADQUARTERS
TRAINING ROOM

BOARD MEETING MINUTES

Board Members Present:
James Stallings, Vice Chairperson
Vic Reynolds (WebEx)
Chris Carr (WebEx)
MG Thomas Carden
Richard Woods
Gary Black
Shawnzia Thomas (WebEx)
Kyle Sapp (WebEx)
Bill Cowsert

Board Members Absent:
Col. Chris Wright
Mark Williams
Kathleen Toomey
Russell McMurry
Alan Powell

Representatives Present:
Lt. Col. Billy Hitchens
Col. Thomas Barnard
Leah Hoffacker
Emily Fish

The Board of Homeland Security held the board meeting on June 1, 2022 at the Georgia Emergency Management and Homeland Security Agency (GEMA/HS) Headquarters in Atlanta, Georgia. 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. Vice Chairperson James Stallings called the meeting to order at 1:33 PM.

All board members are present except Colonel Chris Wright with the Georgia Department of Public Safety, Commissioner Mark Williams with the Georgia Department of Natural Resources, Commissioner Kathleen Toomey with the Georgia Department of Public Health, Commissioner Russell McMurry with the Georgia Department of Transportation, and Representative Alan Powell with the Georgia House of Representatives.

Vice Chairperson James Stallings welcomed everyone to the GEMA/HS Headquarters in Atlanta, Georgia.

Roll Call

Approval of the Minutes:

Vice Chairperson James Stallings presented the minutes of the October 6, 2021 meeting for discussion and approval. Adjutant General Thomas Carden made a motion to approve the minutes. Superintendent Richard Woods seconded the motion. The motion passed unanimously.

Vice Chairperson James Stallings presented the minutes of the December 1, 2021 meeting for discussion and approval. Adjutant General Thomas Carden made a motion to approve the minutes. Superintendent Richard Woods seconded the motion. The motion passed unanimously.

Vice Chairperson James Stallings presented the minutes of the April 6, 2022 meeting for discussion and approval. Commissioner Gary Black made a motion to approve the minutes. Superintendent Richard Woods seconded the motion. The motion passed unanimously.

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

a) GTA Update to the Strategic Plan

David Allen with the Georgia Technology Authority presented on what their agency has been working on regarding the Strategic Plan. David focused on Prevention Goal #2: increase use of technology and cyber-security programs to create a more resilient State.

Harlan Proveaux provided an update on GEMA/HS School Safety efforts. GEMA/HS and the Department of Education are hosting the Georgia School Safety and Homeland Security Conference on June 21st to 23rd in Columbus, Georgia. They have created a new School Safety Plan template that will be presented.

Adjournment:
There being no further business to be brought before the Board, Vice Chairperson James Stallings adjourned the meeting at 2:59 PM.

Official Attachments:

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

BOARD OF HOMELAND SECURITY

WEDNESDAY, JUNE 1, 2022
1:30 TO 3:00 PM
GEMA/HS HEADQUARTERS
TRAINING ROOM

BOARD MEETING ATTENDEES

Board Members:
James Stallings, Vice Chairperson
Vic Reynolds (WebEx)
Chris Carr (WebEx)
MG Thomas Carden
Richard Woods
Gary Black
Shawnzia Thomas (WebEx)
Kyle Sapp (WebEx)
Bill Cowsert

Others Attending:
Chris Allen
David Allen
Anna Braue
Jeff Hodges
Gary Kelley
Tina Piper
Harlan Proveaux
Ashley Seay
Mike Smith

Representatives:
Lt. Col. Billy Hitchens
Col. Thomas Barnard
Leah Hoffacker
Emily Fish

Board of Homeland Security Meeting

AGENDA

June 1, 2022
1:30 - 3:00 P.M.
GEMA/HS Headquarters
Training Room
Atlanta, GA

WebEx/Conference Call
gema.webex.com OR call 1-855-282-6330
Meeting Number: 2436 958 3963
Access Code: HS060122

Agenda Topic	**Speaker**
Call to Order	James C. Stallings, Vice Chairperson GEMA/HS
Roll Call	Harlan Proveaux, GEMA/HS
Approval of Minutes from October 6, 2021	
Approval of Minutes from December 1, 2021	
Approval of Minutes from April 6, 2022	
New Business	
a) GTA Update to the Strategic Plan	David Allen, GTA
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

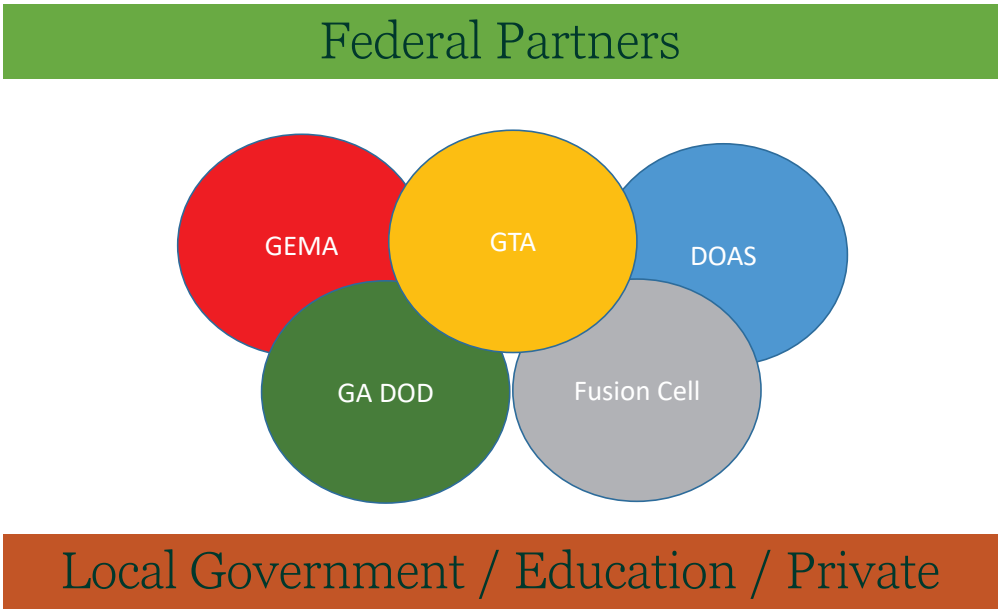
June 1, 2022

Agenda

- GA Cyber Ecosystem and GTA OIS Mission
- Cyber Trends
- Board Mission Area Applicability
- Prevention and Protection
- Response and Recovery
- Next Steps
- Questions / Discussion

- Federal Partners: FBI, DHS, CISA, and DOD provide free resources for prevention and incident response.
- GEMA: Controls overall emergency response and CIKR oversight, to include Cyber severity 1 and 2 incidents. ESF-17 (Cyber)
- 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 provides support to the fusion center for cyber intelligence requirements.
- GA DOD: Maintains resources via the Cyber Protection Team for response to SEV 1 incidents and overall training support.

GA Government Cyber Ecosystem



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

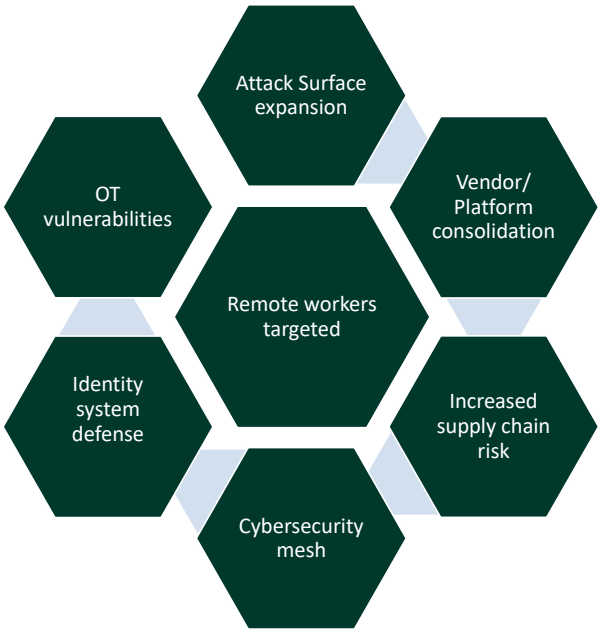
FY22 Accomplishments

- Continued agency assessments and continuous vulnerability management
- Addressed supply chain risk through standardized T&Cs
- Maintained high retention among cyber professionals
- Expanded outreach to underserved agencies and communities
- Increased MFA footprint across the enterprise to include all external user connections/ updated security configurations / standardized geo-blocking across platforms
- Maintained high levels of security awareness training (SAT) and phishing campaigns across the enterprise

- ☑ Expanded Multi-Factor Authentication
- ☑ Segregated and Verified Back-ups
- ☑ Enhanced Detection and Response
- ☑ Improved Advanced Threat Protection
- ☑ Cloud First Strategy

Top Cybersecurity Trends for 2022

- Targeting of remote workers
- Attack surface expansion
- Identity system defense
- Increased supply chain risk
- Vendor / Platform consolidation
- Cybersecurity mesh
- Operational Technology (OT) vulnerabilities



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

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

Prevention and Protection

Prevention/Protection: OIS Outreach

- Bi-monthly Information Security Officer meetings open to all branches, state and local
- OIS actively shares threat intelligence to all state and local partners
  - Bi-weekly report produced by OIS/ESF-17 in cooperation with the GBI
- Cyber awareness presentations to multiple state and local government agencies in 2021/22
  - ESF-17 (1st responder training), GTA Summit, PRIMA conference, USG ISO conference
- 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 2022

Available

New Hire Training Schedule

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

Ongoing Scheduled Training: 2022

Q1 - 4: Phishing campaign – *3 Campaigns each Quarter/1 per month, users who fail phishing must complete auto-enrolled additional training*

- **Q1:** Training modules - *multiple modules on Overall Theme:* ***How to Recognize Phishing Emails***
- **Q2:** Training modules – *multiple modules, Overall Theme:* ***E-mail Attachments and Data Handling***
- **Q3:** Training Modules - *multiple modules on Overall Theme:* ***Social Engineering***
- ***Q4:*** Training Modules – *multiple modules on Overall Theme:* ***Passwords and Remote Working***

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

Upcoming Assessments

REDACTED

Cyber Exercises – 2021 /2022

Completed:

- Cyber Dawg: 13-17 September 2021
- Jack Voltaic: 26 October 2021

Upcoming:

- Cyber Sentinel: 17 August 2022 (Tentative) – ½ day
- Cyber Dawg: 12-16 September – Georgia Cyber Center

Response and Recovery

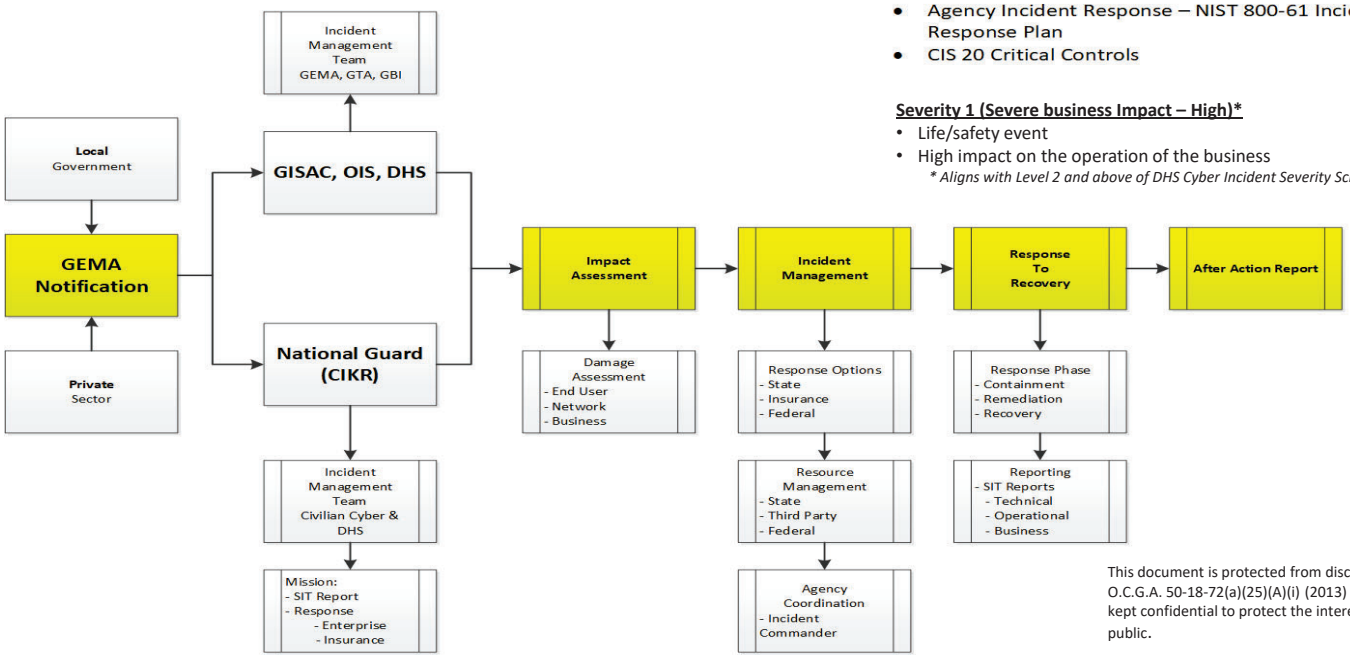
State-Wide Incident Management Process
Escalate to GEMA: Severity 1 Incidents

- National Incident Management System (NIMS)
- Agency Incident Response – NIST 800-61 Incident Response Plan
- CIS 20 Critical Controls

Severity 1 (Severe business Impact – High)*

- Life/safety event
- High impact on the operation of the business

** Aligns with Level 2 and above of DHS Cyber Incident Severity Schema*



GTA Office of Information Security (OIS) Incident Response Summary

REDACTED

Cyber Insurance

REDACTED

Next Steps

FY23 Way Ahead

- Shifting critical applications to the cloud
- Expanding cybersecurity team (adding 7 for 20 total in FY23)
- Expanding threat hunting / SIEM capabilities
- Implementation of zero trust methodologies / Privileged Access Management
- Expansion of EDR footprint
- Continued investment in continuous vulnerability management

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