Georgia Emergency Management &
Homeland Security Agency

Georgia HB 156
Cyber Incident Reporting Requirements

Chris Allen
Homeland Security
Special Projects Coordinator

Jonathan Baugh
GTA Cyber Security Analyst
ESF 17 Lead

GEMA/HS Cyber Security

- Cyber Security is a statewide priority for Georgia

- HB 156
  - Why should you report? (besides it's the law!)
  - Who needs to report?
  - When to report?
  - What needs to be reported?
  - How to report a Cyber Incident?

Who We Are

- **Mission**
  - The mission of the Georgia Emergency Management and Homeland Security Agency is to facilitate the protection of life and property against man-made and natural disasters by directing the state's efforts in the areas of prevention, preparedness, mitigation, response, and recovery.
- **Vision**
  - The vision of the Emergency Management and Homeland Security Agency is to create a safer Georgia by providing strong leadership and promoting excellence.

Georgia Hazard Analysis

- Floods
- Wildfires
- Droughts
- Earthquakes
- Technological & Man-Made Disasters & events
- Tropical Systems – Including Hurricanes and Tropical Storms
- Terrorism
- Winter Storms
- Evacuee Support

Disaster History in Georgia
Why We Are Here

Georgia has experienced
20 major disasters in the past
two decades and
46 since 1953.

State of Georgia
Major Disaster Declarations

- 1953 Tornado
- 1954 Tornado
- 1961 Floods
- 1963 Severe Storms
- 1964 Hurricane Dora
- 1964 Flooding
- 1966 Flooding
- 1973 Tornadoes
- 1973 Tornadoes Flooding
- 1974 Tornadoes
- 1975 Tornadoes, Heavy Winds
- 1976 Severe Storms, Flooding
- 1977 Shrimp Loss Due to Cold Weather
- 1977 Dam Collapse, Flooding
- 1990 Flooding, Severe Storm
- 1990 Flooding, Severe Storm
- 1991 Flooding, Severe Storm
- 1992 Heavy Rain, High Winds, Tornadoes
- 1993 Tornadoes, High Winds, Heavy Rain
- 1994 Severe Storm, Tornadoes, Flooding
- 1994 Tornadoes
- 1994 Heavy Rains, Tornadoes, Flooding
- 1995 Hurricane Opal
- 1995 Severe Storms, Tornadoes
- 1998 Severe Storms, Tornadoes, Floods
- 1999 Severe Storms
- 2000 Winter Storm
- 2000 Tornadoes
- 2004 Hurricane Ivan
- 2004 Tropical Storm Frances
- 2007 Severe Storms and Tornadoes
- 2008 Severe Storms and Tornadoes
- 2008 Severe Storms and Flooding
- 2009 Severe Storms, Flooding, Tornadoes, and Straight-Line Winds
- 2009 Severe Storms and Flooding
- 2011 Tornadoes
- 2014 Ice/Winter Weather
- 2015 Ice/Winter Weather
- 2015 Flooding
- 2016 Hurricane Matthew
- 2017 January 2nd Tornadoes
- 2017 January 21st Tornadoes
- 2017 Hurricane Irma
- 2018 Hurricane Michael
- 2019 Hurricane Dorian
- 2020 COVID-19 Pandemic

Notable State of Georgia Disaster Declarations

- 1975 Tornadoes
- 1977 Drought
- 1984 Severe Storms, Tornadoes
- 1993 Severe Snowfall, Winter Storms
- 1994 Floods
- 1999 Hurricane Floyd
- 2005 Hurricane Katrina Evacuation
- 2011 Tornado Outbreak
- 2017 Hurricane Irma
- Hurricane Michael
- 2020 COVID-19 Pandenic

Hurricane Floyd

1993 Winter Storm

Six Phases of Cyber Incident Responce

Five Phases of Comprehensive Emergency Management

- Prevention - To stop an incident from occurring
- Preparedness – To Respond
- Response – To Emergency
- Recovery – Short and Long Term
- Mitigation – Long Term

Cyber Incidents / HB 156 Overview

- Georgia's expanding prioritization of Cyber Security
  - Georgia Cyber Center
  - Emergency Support Function 17 - Cyber
- HB156's call to report all cyber incidents to GEMA/HS
- How to Report to GEMA
  - GTA vs. non GTA
- Why to Report to GEMA
  - Critical + Protected + Prevention

HB 156 Analysis

- Definitions -
- Agency means:
  - (A) The executive, judicial, or legislative branch of this state and any department, agency, board, bureau, office, commission, public corporation, and authority thereof;
  - (B) Every county, municipal corporation, school district, or other political subdivision of this state;
  - (C) Every department, agency, board, bureau, office, commission, authority, or similar body of each such county, municipal corporation, or other political subdivision of this state; and
  - (D) Every city, county, regional, or other authority established pursuant to the laws of this state.

HB 156 Analysis

- Such term shall not include any county, municipal corporation, or public corporation or any authority of a county, municipal corporation, or public corporation when such county, municipal corporation, public corporation, or authority is acting in the capacity of a provider of wholesale or retail electric or gas service or in the capacity of a conduit through which a municipal corporation furnishes electric or gas service.
- 2) 'Utility' means any publicly, privately, or cooperatively owned line, facility, or system for producing, transmitting, or distributing power, electricity, light, heat, or gas.

HB 156 Analysis

- (b)(1) Except as provided in paragraph (2) of this subsection, every agency shall report to the director of emergency management and homeland security, or his or her designee, any cyber attack incident, data breach, or identified use of malware on an agency or computer or network determined by the director to be the type of cyber attack, data breach, or use of malware to create a life-safety event, substantially impact the security of data and information systems, or affect critical systems, equipment, or service delivery.
- AKA: “Every Agency shall report to GEMA/HS any cyber incident on an agency.”

HB 156 Analysis

- (2) The reporting requirements of paragraph (1) of this Code section shall be satisfied if:
  - (A) The cyber attack incident, data breach, or identified use of malware upon an agency is of a nature required to be reported to the United States government or any agency thereof or the agency elects to report such cyber attack incident, data breach, or identified use of malware to the United States government or any agency thereof; and
  - (B) Within two hours of making such report to the United States government or any agency thereof, the agency provides substantially the same information to the director of emergency management and homeland security or his or her designee.

HB 156 Analysis

- (3) The director of emergency management and homeland security shall, subject to approval by the Governor, promulgate rules and regulations specifying the reporting mechanism for making a report under paragraphs (1) and (2) of this subsection and the required information and time frame for making a report under paragraph (1) of this subsection.
  - "GTA Reporting vs. Non GTA Reporting"
  - Two (2) Hours from initial incident detection
  - Cat I, II, & Cat 3 Compromises

HB 156 Analysis

- (c) Every utility shall report to the director of emergency management and homeland security, or his or her designee, any cyber attack incident, data breach, or identified use of malware on a utility computer or network as such information is required to be reported to the United States government or any agency thereof. Within two hours of making such report to the United States government or any agency thereof, the utility shall provide substantially the same information to the director of emergency management and homeland security or his or her designee; provided, however, if such information is prohibited under any federal law, rule, or regulation from being disseminated, the utility shall provide such information upon the expiration or lifting of such prohibition.

HB 156 Analysis

- (d) Any reports or records produced pursuant to this Code section shall not be subject to public inspection or disclosure under Article 4 of Chapter 18 of Title 50.
- (e) Nothing in this Code section shall relieve any agency or utility of any duty that may exist under law to notify any person impacted by a cyber attack incident, data breach, or identified use of malware, including, but not limited to, any notice required under Article 34 of Chapter 1 of Title 10.
- End of relevant cyber language

Reporting Process

- What to report
  - Severity I, II, and Compromised credentials
  - Not your daily MacAfee Scan
- When to report
  - Within 2 hours of initial detection
- How to report
  - State Warning Point 1-800-TRY-GEMA
  - Web Portal Coming Soon
- What happens after you report and ask for state help?
  - GTA vs. DOD

Key Takeaways

- Why to report (Besides it's the law!)
- Who should report?
- When to report?
- What to report?
- How to report?

GEMA/HS

- Questions?

Contact Us!

- Chris Allen
- Homeland Security Special Project Coordinator
- Christopher.allen@gema.ga.gov

- Jonathan Baugh
- ESF – 17 (Cyber) Lead + GTA Cyber Security Analyst
- Jonathan.baugh@gta.ga.gov

- Georgia School Safety & Homeland Security Conference
- June 21 – 23, 2022
- Columbus, Georgia