



U.S. Department of Education  
Office of Safe and Drug-Free Schools  
Emergency Management for Higher Education



FY 2009 Final Grantee Meeting ♦ Philadelphia, PA ♦ August 5 – 6, 2010

---

## Cyber Security

**James A. McGee, MS**

Security Consultant

The University of Southern Mississippi

National Center for Spectator Sport Safety and Security (NCS4)

118 College Drive #5193, Hattiesburg, MS 39406

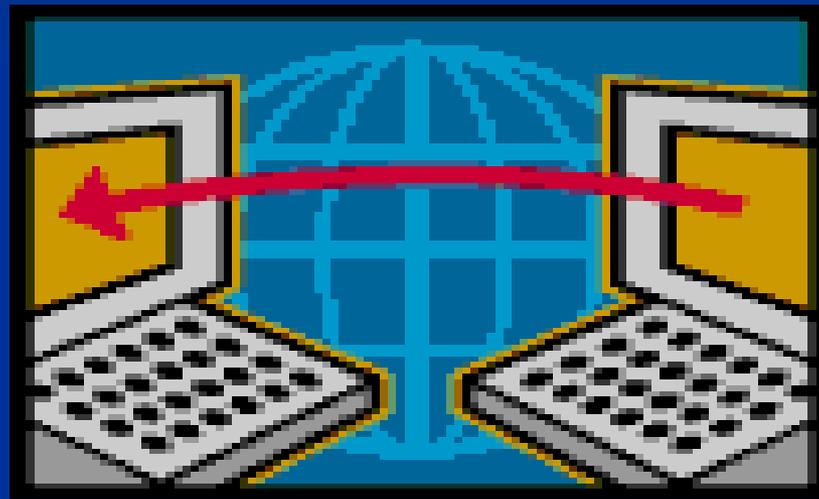
Phone: (601) 266-6734      Email: [James.A.McGee@usm.edu](mailto:James.A.McGee@usm.edu)

*James A. McGee, MS* has twenty-five combined years of law enforcement experience, twenty-one years as a Special Agent with the Federal Bureau of Investigation (FBI) and a Master of Science in Criminal Justice from Virginia Commonwealth University, Richmond, Virginia. His experience includes ten years in criminal justice administration and project management as an FBI Supervisor. In addition, Mr. McGee has sixteen years of experience addressing international security issues, counterterrorism investigations, crisis management, critical infrastructure protection/risk assessments, and homeland security initiatives. He is currently employed as a Security Consultant with The University of Southern Mississippi National Center for Spectator Sport Safety and Security and as an Adjunct Professor with the Tulane University Department of Homeland Security Studies. Mr. McGee frequently teaches for the United States Department of State Anti-Terrorism Assistance Program. Further, he has been designated as an expert witness in security issues regarding critical infrastructure protection, specifically venues of mass gatherings of people.

# Cyber Security

FY 2009 EMHE Final Grantee Meeting  
Philadelphia, Pennsylvania

August 5-6, 2010



Presented by:

James A. McGee – National Center for  
Spectator Sport Safety and Security (NCS4)

# OVERALL GOAL

- To review, improve, and fully integrate campus-based emergency plans at The University of Southern Mississippi into a seamless, all hazards emergency management plan that is communicated to, and practiced by its faculty, staff, and students.



# Planning

- Identify and understand all threats, risks, and hazards to the USM campus communities.
- Develop an integrated, all-hazards emergency management plan that is NIMS compliant and comprehensive.
- The emergency management plan and personnel will meet the emergency management-related needs of persons with disabilities and special needs.



# Taskings

- Organize Working Groups based on subject matter expertise.
- Each Working Group will gather relevant plans from the USM and local Emergency Response community.
- The plans will be reviewed and improved as needed.



# Taskings (Cont'd.)

- In cases where a plan does not exist, one will be written.
- Once all relevant plans have been obtained they will be fully integrated into a campus-based Emergency Management Plan.



# Training

- An informed, practiced, NIMS-compliant staff that is well-prepared to handle emergency management duties.
- The campus community will understand its role and responsibilities in emergency management.



# Exercises

- Tabletop (TTX) – Scenario driven to test plans and enhance campus awareness of roles and responsibilities during an emergency. Conducted in a round table setting.
- Three TTXs beginning Fall 2009. Variety of scenarios targeting different communities on campus.



# Exercise Challenges

- Select and confirm a proposed date for the TTXs to be delivered at USM.
- Who will be invited to attend?
- Does a USM Plan currently exist?
- The need for a USM Plan to be in place so that it can be tested during the TTX.



# Table Top Exercises

Delivery dates:

- TTX I – Pandemic Scenario (01/31/2010)
- TTX II – Cyber Security (03/09/2010)
- TTX III – Severe Weather/Special Needs Community (08/11/2010)



# TTX Content/Logistics

- Exercise Scenario Development
- Situation Manual (SITMAN);  
Facilitator/Participant Guides
- Exercise Rules
- Exercise Objectives
- Exercise Schedule/3 hour duration
- 3 Modules/Scenario Injects
- Power Point Delivery



# Cyber Security Exercise Rules

- Scenario depicts a plausible cyber security event
- No trick questions or “hidden” agendas
- Players have no previous knowledge of the scenario, and will receive information at the same time
- Players will respond using existing plans, procedures and other response resources
- Decisions are not precedent-setting and may not reflect your organization’s final position on a given issue



# Exercise Objectives

- Examine the capabilities of USM to prepare for, protect from, and respond to the effects of cyber attacks.
- Exercise senior leadership decision making and interagency coordination of incident responses in accordance with the USM Cyber Response Plan.
- Validate information sharing relationships and communications paths for the collection and dissemination of cyber incident situational awareness, response, and recovery information.
- Exercise intra-governmental (Federal-State) coordination and incident response.
- Identify policies/issues that hinder or support cyber security requirements.



# Exercise Objectives (Cont'd.)

- Identify public/private interface communications and thresholds of coordination to improve cyber incident response and recovery, as well as identify critical information sharing paths and mechanisms.
- Identify, improve, and promote public and private sector interaction in processes and procedures for communicating appropriate information to key stakeholders and the public.
- Identify cyber physical interdependence of infrastructure of real world economic and political impact.
- Raise awareness of the economic and national security impacts associated with a significant cyber incident.
- Highlight available tools and technology with analytical cyber incident response and recovery capability.



# Cyber Security Scenario

The exercise simulates a sophisticated cyber attack campaign through a series of modules directed against critical infrastructures. The intent of these modules is to highlight the interconnectedness of cyber systems with the physical infrastructure and to exercise coordination and communication between the public and private sectors.



# Cyber Security Scenario (Cont'd.)

The exercise is a simulated event with no real world effects on, tampering with, or damage to any critical infrastructure. While the scenario is based on hypothetical but possible situations, they are not intended as a forecast of future terrorist-related events.

The collective modules have three major adversarial objectives:

- To disrupt specifically targeted critical infrastructures through cyber attacks
- To hinder the University's ability to respond to the cyber attacks
- To undermine public confidence in the University's ability to provide/protect services



# Sample Scenario Injects

- The following incidents involving disruptions to cyber security at USM have been reported:
  - Hackers recently broke into the USM computer database, which could potentially compromise student, faculty and staff records.
  - Upon consulting with the Multi State Information Sharing and Analysis Center (MS-ISAC), it was revealed that six other universities were having similar problems.
  - Reports that certain USM on-line service support systems (everything from SOAR to financial aid) are down or behaving erratically due to what appears to be a massive computer virus attack.
  - The “hacktivists” specifically targeted several critical infrastructure sectors, along with state and federal agencies, the media, and universities.
  - By generating counterfeit digital certificates, the “hacktivists” directed unknowing USM web users to “spoofed” websites where funds were extorted and personal information was mined.



# Sample Scenario Injects (Cont'd.)

- Coordinated attacks on domain name servers and telecommunications router infrastructure resulted in a distributed denial of service and unreliable telephony. Users were intermittently unable to access websites, send email, and make phone calls. Victims of the attack were forced to explore alternative methods of communication during the disruptions.
- The USM Chief Security Officer (CSO) has received e-mail threats and false Amber Alerts have been broadcast. The series of suspicious events compelled the USM CSO to request activation of the State's Emergency Operations Center.



# Module

## Key Discussion Questions

- What kind of information is available to faculty, staff, students, and parents about an attack to the cyber system?
- Have faculty, staff, community and emergency response partners been involved in providing input and feedback for crisis planning for schools?
- Will faculty and staff play a role in the incident command structure once the Incident Command System (ICS) is activated during an emergency? If so, what is the role?
- Is the USM current emergency response plan suited for a cyber attack?
- Is there a communication plan for keeping faculty, staff and students informed of decisions regarding attacks to the cyber system?



# Key Discussion Questions (Cont'd.)

- Does the university have firewalls and countermeasures in place to protect the cyber system?
- Does the university plan to maintain educational operations in the case of a large scale cyber attack? If so, what plan is in place for maintaining continuity of instruction/business?
- Does the university have established communication protocols with community and emergency response partners during a massive cyber attack?
- What is the university's plan to communicate with media for latest information dissemination?
- What is the university's plan to communicate with emergency response partners during a cyber attack of this nature?



# Exercise Debriefing Questions

- Does the USM emergency management plan adequately address key issues, such as faculty and staff training in the event of a cyber attack?
- What problems did you identify in the emergency management procedures that could hinder emergency management efforts associated with a cyber attack?
- Does the USM emergency management plan adequately address key issues faced during a cyber attack, including continuity of business operations (e.g., payroll) and student accounts?



# Exercise Debriefing Questions

## (Cont'd.)

- Does the USM emergency management procedures properly coordinate communication as an emergency response activity among colleges, students, faculty, staff and community and emergency response partners during a cyber attack? In your opinion, what can be done to improve communication during an emergency situation such as the cyber attack scenario presented in the exercise?
- Does the emergency management plan include partnerships with local and regional partners ensuring service and support during a cyber attack?
- In what ways were/will parents be engaged as stakeholders during the response to cyber attack?



# Exercise Debriefing Questions

## (Cont'd.)

- Is there adequate support for students, faculty, and staff before, during, and after a mass cyber attack? If not, what activities and partnerships did the team identify to enhance assistance to faculty, staff, and students?
- Overall, what activities hastened recovery of the USM cyber system? What strategies prevented a greater prevalence of disruption? What are lessons learned for responding to future cyber attacks? What activities were the most helpful for recovering from the cyber attack?
- What activities or processes were identified as gaps or weaknesses and will be addressed in future efforts?



# Lessons Learned

- Identify a critical time period after which data loss and malfunction of specific systems would be catastrophic, and develop a contingency plan that addresses continuing university academics and business operations in the event of a cyber outage.
- Recognize if there is no formal communication plan with other universities for this type of scenario, and work to develop one.
- Conduct an informational campaign so students and staff know where to go to get information during an emergency, and establish emergency communication procedures and back-ups in the event of an outage, including:
  - An off-campus web site that is updated by a third party.
  - A phone line that can be called for up-to-date information.



# Lessons Learned (Cont'd.)

- Conduct training across campus for students, faculty, and staff around the following topics:
  - The dangers of a cyber outage, especially considering the extent of dependency on computers and networks, and the widespread effects one would cause.
  - How cyber breaches can be prevented (e.g. antivirus software) and awareness that any machine can be compromised, not just servers, to create a system-wide attack.
- Conduct a vulnerability assessment for the existence and location of classified research data on campus.
- Develop standard policies and procedures for servers across campus, especially those outside the IT department's control.
- Consider developing a university working group to address cyber outage issues.



# Cyber Security TTX

- Available via the Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center
- Facilitator/Participant Manuals
- TTX Power Point



# Questions

