Cyber Security Training and Exercise Program

State of Nevada

CIAS

UTSA

Overview

- Background
- CIAS Program
- Plan and timing
- Next Steps
- Discussion

Bottom Line

- Nevada competed for and secured this program
- Community Cyber Security Program
  - Multi-month program of courses, exercises, and workshops
  - No financial cost to the state / community
- Program Goals
  - Forge public-private cybersecurity partnership
  - Raise awareness throughout community
  - Enhance collaboration to better protect citizens and infrastructure
  - Seed success for the future
- Success lies in participation
  - Leadership and decision makers are key

Executive support and involvement is crucial

National Problem, Local Solutions

"The national security and economic health of the United States depend on the security, stability, and integrity of our Nation's cyberspace, both in the public and private sectors. The President is confident that we can protect our nation's critical cyber infrastructure while at the same time adhering to the rule of law and safeguarding privacy rights and civil liberties…"

John Brennan
Assistant to the President
for Counterterrorism and Homeland Security,
Feb 2009

Center for Infrastructure Assurance and Security

- Non-profit Center at The University of Texas at San Antonio
  - Founded in 2001
- Focus areas
  - Cyber Security Training: multi-level courses, boot-camps and workshops
  - Cyber Defense Competition Programs
  - Infrastructure Assurance Programs: combined exercise & training programs
- Resources
  - Grant funded (DHS, DoD)
  - Other as arranged with public and private entities

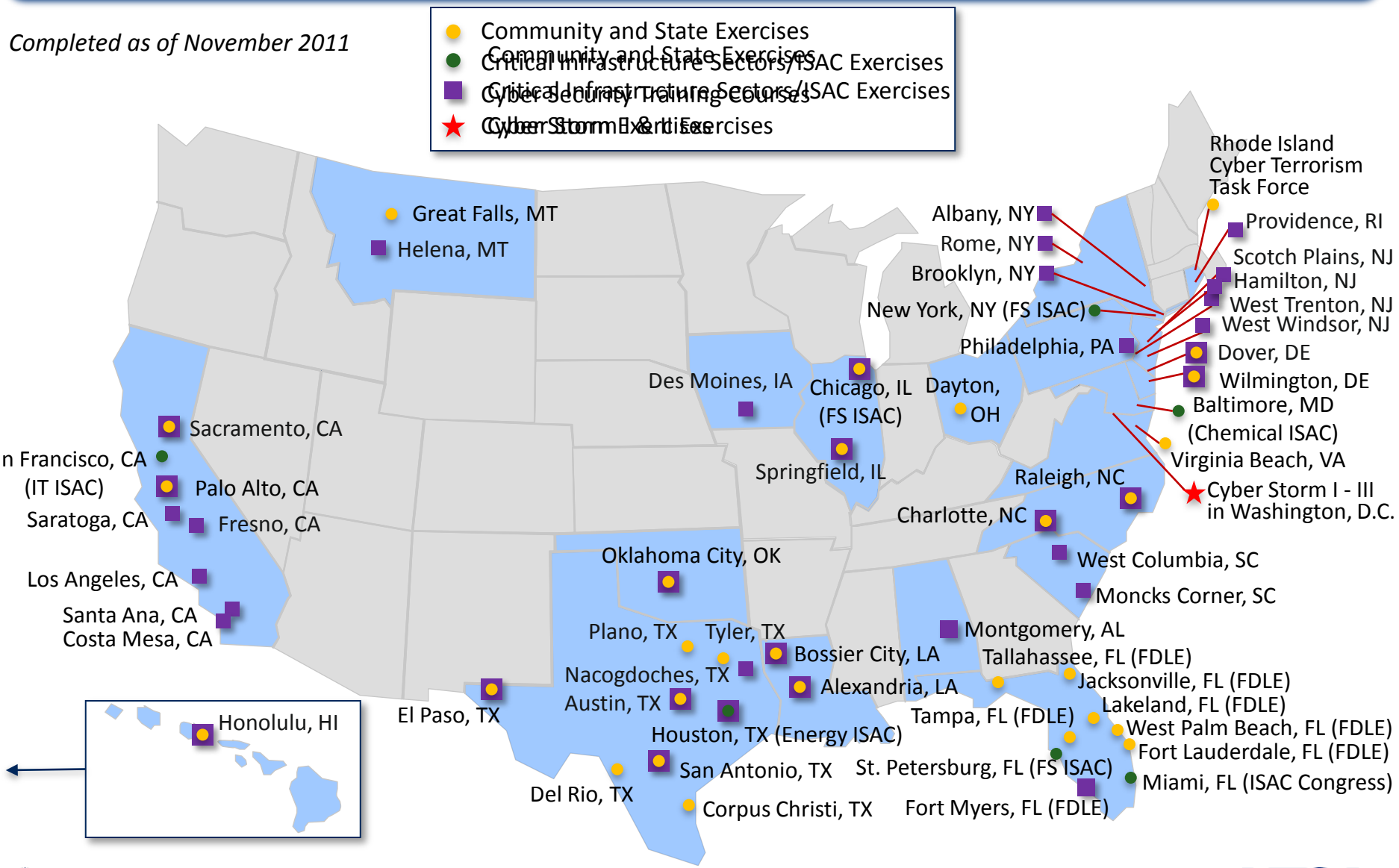
UTSA is a NSA / DHS National Center of Academic Excellence in Information Assurance Education

CIAS

UTSA

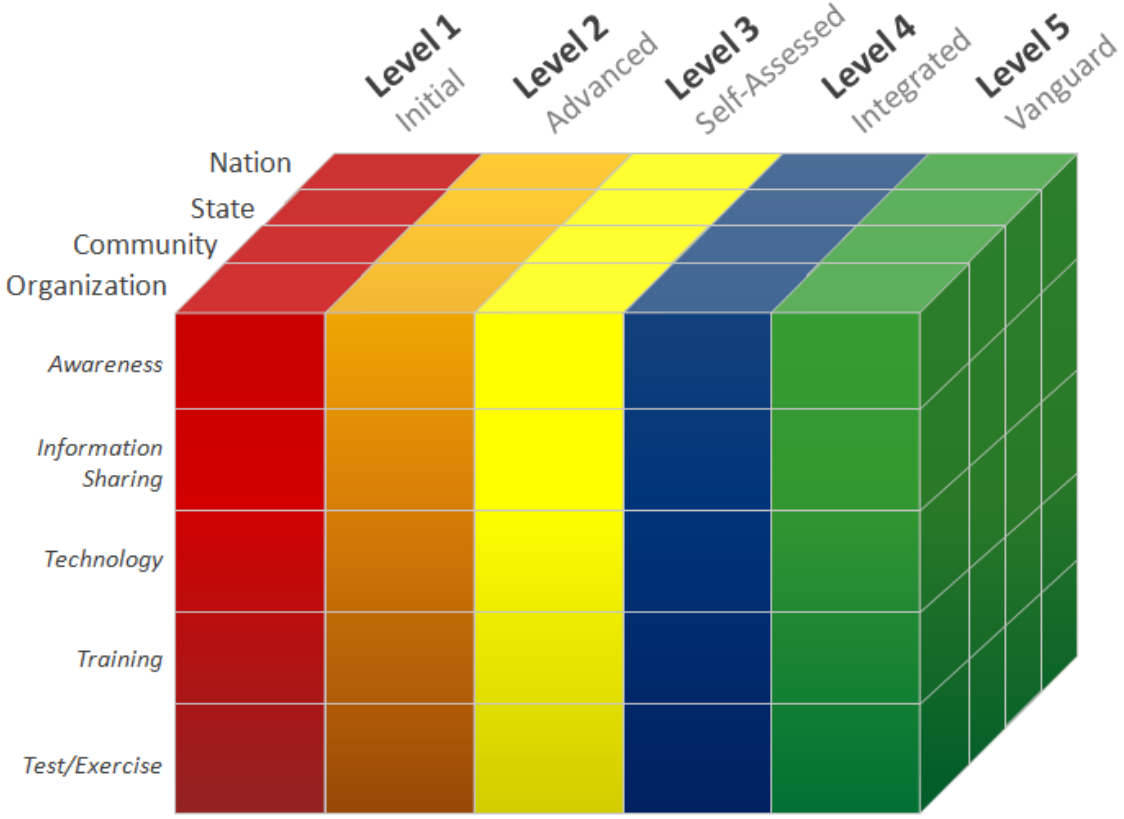
Completed Training and Exercises

Completed as of November 2011



Community Cyber Security Maturity Model

- Standard developed by the CIAS
  - Based on experience across the nation
  - Development supported by Congress and DHS
- Multi-dimensional
  - Collaboration is key
- Provides
  - Common reference
  - Roadmap
  - Foundation for success



CIAS

UTSA

Community Cyber Security Maturity Model

LEVEL 1
Initial

- Minimal cyber awareness
- Minimal cyber info sharing
- Minimal cyber assessments and policy & procedure evaluations
- Little inclusion of cyber into Continuity of Operations Plan (COOP)

LEVEL 2
Advanced

- Leadership aware of cyber threats, issues and imperatives for cyber security and community cooperative cyber training
- Informal info sharing/ communication in community; working groups established; ad-hoc analysis, little fusion or metrics; professional orgs established or engaged
- No assessments, but aware of requirement; initial evaluation of policies & procedures
- Aware of need to integrate cyber security into COOP

LEVEL 3
Self-Assessed

- Leaders promote org security awareness; formal community cooperative training
- Formal local info sharing/cyber analysis. initial cyber-physical fusion; informal external info sharing/ cyber analysis and metrics gathering
- Autonomous tabletop cyber exercises with assessments of info sharing, policies & procedures, and fusion; routine audit program; mentor externals on policies & procedures, auditing and training
- Include cyber in COOP; formal cyber incident response/recovery

LEVEL 4
Integrated

- Leaders and orgs promote awareness; citizens aware of cyber security issues
- Formal info sharing/ analysis, internal and external to community; formal local fusion and metrics, initial external efforts
- Autonomous cyber exercises with assessments of formal info sharing/local fusion; exercises involve live play/metrics assessments
- Integrate cyber in COOP; mentor externals on COOP integration; formal blended incident response and recovery

LEVEL 5
Vanguard

- Awareness a business imperative
- Fully integrated fusion /analysis center, combining all-source physical and cyber info; create and disseminate near real world picture
- Accomplish full-scale blended exercises and assess complete fusion capability; involve/ mentor other communities/entities
- Continue to integrate cyber in COOP; mentor externals on COOP integration; formal blended incident response and recovery

CIAS

UTSA

Community Cyber Security Maturity Model

LEVEL 1 Initial	LEVEL 2 Advanced	LEVEL 3 Self-Assessed	LEVEL 4 Integrated	LEVEL 5 Vanguard
• Minimal cyber awareness • Minimal cyber info sharing • Minimal cyber assessments and policy & procedure evaluations • Little inclusion of cyber into Continuity of Operations Plan (COOP)	• Leadership aware of cyber threats, issues and imperatives for cyber security and community cooperative cyber training • Informal info sharing/ communication; community; groups established; ad-hoc analysis, little fusion or metrics; professional orgs established or engaged • No assessments, but aware of requirement; initial evaluation of policies & procedures • Aware of need to integrate cyber security into COOP	• Leaders promote org security awareness; formal community cooperative training • Formal local info sharing/cyber analysis. initiation; cyber-physical fusion; formal external info sharing/ cyber analysis; metrics gathering • Autonomous tabletop cyber exercises with assessments of info sharing, policies & procedures, and fusion; routine audit program; mentor externals on policies & procedures, auditing and training • Include cyber in COOP; formal cyber incident response/recovery	• Leaders and orgs promote awareness; citizens aware of cyber security issues • Formal info sharing/ analysis, internal and external to community; formal local fusion and metrics, initial external • Autonomous cyber exercises with assessments of formal info sharing, fusion; exercises involve live play/metrics assessments • Integrate cyber in COOP; mentor externals on COOP integration; formal blended incident response and recovery	• Awareness a business imperative • Fully integrated fusion /analysis center, combining all-source physical and cyber info; create and disseminate near real world picture • Accomplish full-scale blended exercises and assess complete fusion capability; involve/ mentor other communities/entities • Continue to integrate cyber in COOP; mentor externals on COOP integration; formal blended incident response and recovery

Phase One

Phase Two

Phase Three

Phase Four

CIAS

UTSA

Phase One – Approach

- Phase centers on three tabletop exercises (TTXs)
  - TTX 1 – 100-person community cross-sector
  - TTX 2 – 60-person community sector-based
  - TTX 3 – concurrent 30-person state and two 15-person communities
- Transition events – before and after each exercise
  - Planning conferences, After Action Report workshops
  - Training courses and seminars throughout
- Phase emphasis on foundation of awareness
  - Enhance awareness of threats, issues, vulnerabilities and actions
  - Examine imperatives for policies, procedures, training and awareness
  - Discuss and explore internal / external information sharing

Phase One – Program Elements

Community Exercise 1

1. Initial Contact Meeting
2. Leading Cyber Security ourse & Initial Planning Conference
3. Final Planning Conference
4. Community Cyber Security Exercise
5. After Action Report Workshop
6. Voice and Data Security Course
7. On-site Cyber Security Solutions Workshops

Community Exercise 2

8. Initial Planning Conference & Leading Cyber Security Course (2nd Offering)
9. Final Planning Conference
10. Community Cyber Security Exercise
11. After Action Report Workshop

State & Community Exercise 3

12. Initial Planning Conference
13. Final Planning Conference
14. State and Community Cyber Security Exercise
15. After Action Report Workshop

CIAS

UTSA

Phase One – Program Element Phasing

Community Exercise 1

1. Initial Contact Meeting
2. Leading Cyber Security Course & Initial Planning Conference
3. Final Planning Conference
4. Community Cyber Security Exercise
5. After Action Report Workshop
6. Voice and Data Security Course
7. On-site Cyber Security Solutions Workshops

Community Exercise 2

8. Initial Planning Conference & Leading Cyber Security Course (2nd Offering)
9. Final Planning Conference
10. Community Cyber Security Exercise
11. After Action Report Workshop

State & Community Exercise 3

12. Initial Planning Conference
13. Final Planning Conference
14. State and Community Cyber Security Exercise
15. After Action Report Workshop

- Events separated 3-4 weeks
- Communities staggered 2-3 weeks

CIAS

UTSA

Phase One – Exercises

Community Exercise 1

1. Initial Contact Meeting
2. Leading Cyber Security Course & Initial Planning Conference
3. Final Planning Conference
4. Community Cyber Security Exercise
5. After Action Report Workshop
6. Voice and Data Security Course
7. On-site Cyber Security Solutions Workshops

Community Exercise 2

8. Initial Planning Conference & Leading Cyber Security Course (2nd Offering)
9. Final Planning Conference
10. Community Cyber Security Exercise
11. After Action Report Workshop

State & Community Exercise 3

12. Initial Planning Conference
13. Final Planning Conference
14. State & Community Cyber Security Exercise
15. After Action Report Workshop

CIAS

UTSA

Phase One – Proposed Timeline

Community Exercise 1

1. Initial Contact Meeting
2. Leading Cyber Security Course & Initial Planning Conference
3. Final Planning Conference
4. Community Cyber Security Exercise (May- Jun 2012)
5. After Action Report Workshop
6. Voice and Data Security Course
7. On-site Cyber Security Solutions Workshops

Community Exercise 2

8. Initial Planning Conference & Leading Cyber Security Course (2nd Offering)
9. Final Planning Conference
10. Community Cyber Security Exercise (Oct-Nov 2012)
11. After Action Report Workshop

State & Community Exercise 3

12. Initial Planning Conference
13. Final Planning Conference
14. State & Community Cyber Security Exercise (Feb-Mar 2013)
15. After Action Report Workshop

- Program spans approximately 14 months
  - Launch – February 2012
  - Completion – March 2013

Phase One – Near Term…

Community Exercise 1

1. (Feb 2012)
   - Initial Contact Meeting(s)
2. (Mar-Apr 2012)
   - Leading Cyber Security course – 3 hours
   - Initial Planning Conference – 2 hours
3. (Apr-May 2012)
   - Final Planning Conference – 1-2 hours
4. (May-Jun 2012)
   - Tabletop # 1 Exercise – full-day, discussion-based exercise

5-7. (Jul-Aug 2012)
   - AAR Workshop – 3 hours
   - Voice and Data Security course and lab – 4 days
   - On-Site Cyber Security Solutions Workshop – on-site visits over 3-days, 2 hours each

Target Audience

- Leadership
  - Operational executives
  - Policy makers
  - Resource authorities
  - Information security leadership
- Community public and private organizations
  - Infrastructure, business, government, services
  - Inclusive not exclusive
- Not the “Choir”

Typical Participants

- City, County, some State Officials
- Critical Infrastructure Providers – Public and Private
  - Power, Water, Telecom, ISPs, Transportation (Air, Rail, Water, Road)
- Emergency Services, First Responders, Disaster Preparedness
  - Law Enforcement, Fire / Rescue, Medical
  - Emergency Operations Centers, Fusion Centers
- Military – Active, Guard, Reserve Commanders and Directors
- Public Schools, Colleges, Universities
- Major commercial community organizations
  - Services, financial, industrial, healthcare
- Chambers of Commerce / Economic Development Organizations
- Visitors – Invited VIPs (Senators, Representatives, Governor)
- Media – Involvement determined by community
  - Public Information Officers

Not an “IT Exercise” - Designed for decision makers

Program Considerations

- Points of Contact
  - State POC
  - Community Champions and POCs
- Resources
  - CIAS provides
    - All exercise, training and workshop materials
    - Exercise Directors, Facilitators and Instructors
    - Locally catered lunch during exercises
  - States and communities provide
    - Exercise, training, workshop and meeting venues
    - Attendee invites and coordination
    - Administrative support for exercise registration
    - State and community personnel travel if required

Next Steps

- Get the word out, involve Leadership ASAP
- Identify / confirm POCs
  - State
  - Community
- Schedule / Conduct Initial Contact Meeting(s)
  - Location
  - Date / Time
  - Attendee list
- Additional contact meetings needed / desired?
- Any schedule constraints known thus far?
- Media?

Lessons from Past Events

- Employees and citizens are the on the front lines of defense
  - Technology can't replace a well trained and educated community and workforce
- Community coordination and communication is a force multiplier
  - Starting a dialogue is the first step in determining what is pertinent to communicate
  - There are often others who may want to know about a cyber event
  - Information sharing relationships enable early indications and warnings
- Increased awareness of community interdependencies is essential including:
  - Agencies and organizations interdependencies
  - Links between critical infrastructures
  - Reliance on vulnerable networks
- The blending of cyber and physical threats can and have been employed
  - Each can multiply the effects and provide an opportunity for the other
- The military community isn't an "island"
  - Everyone, both on and off a military installation, relies on community infrastructures

National Problem, Local Solutions

"I truly believe that as a nation, and as a society, we will rise to this complex challenge if we commit to engaging in – and sustaining – a broad public conversation about the shared responsibility for securing cyberspace. It must become a common value for all Americans that responsibility for cybersecurity begins with each individual user and extends out to every business, school, and other civic and private enterprise. All of us, from the most casual users to the most highly-trained experts, share in the responsibility to learn about cybersecurity and to do more, individually and collectively"

Secretary Janet Napolitano

U.S. Department of Homeland Security

Remarks to UC Berkeley College of Engineering,

Berkeley, California, April 2011

CIAS Points of Contact

Project Lead

Stephanie Ewing-Ottmers

stephanie.ewingottmers@utsa.edu (210) 458-2167

Technical Lead

Paul Fletcher

paul.fletcher@utsa.edu (210) 458-2142

CIAS Associate Director

Larry Thompson

larry.thompson@utsa.edu (210) 458-2162

http://cias.utsa.edu