Investment #3

Investment Information - Investment #3

Investment Name: Cyber Security - Critical Infrastructure

Investment Phase: New

Multi-Applicant Investment: No

I. Overview - Investment #3

I.C. - Funding Program

Designation	Program	Funding Amount
Primary:	SHSP	$467,500
Secondary:	No Secondary Source	

*** I.D. - Capabilties Building**

Building new capabilities.

I.E. - Investment description

Provide a description of this Investment, including the planning, organization, equipment, training, and/or exercises that will be involved. (2,500 char. max)

Technology is a fundamental component of all lines of business. Technology is used to power the electrical grid, to supply water, to maintain sewer systems, to maintain key businesses, to provide hospital care, to insure reliable food supplies, to regulate the flow of traffic, and to provide communications for all aspects of government, including first responders, during an emergency. The security and reliability of the technological components of critical infrastructure is essential.

Nevada recognized the importance of building an effective cyber response. Through cyber seminars, a tabletop exercise and institutional understanding, the Chief Information Officers and lead information security personnel of various cities, counties and state agencies in Nevada discussed their top cyber security concerns and how best to improve the cybersecurity posture for Nevada's government entities. This group, The Nevada Cybersecurity Committee (NCC), included participants from the cities of Las Vegas, Henderson, Reno, Sparks, and North Las Vegas, the counties of Clark and Washoe, the State Departments of Information Technology and Public Safety, the Clark County School District and the Las Vegas Metropolitan Police Department. This group is responsible for over 90 percent of the statewide population.

The Nevada Cybersecurity Committee identified 65 cybersecurity initiatives which they classified and prioritized info five broad areas: 1) cyber assessments/incident response, 2) access control; 3) availability of critical systems; 4) security awareness; 5) data security/confidentiality. Subcommittees of the NCC produced project proposals. The three highest priority areas are included in this investment justification.

II. Baseline - Investment #3

II.A. - Goals and Objectives

Identify the goals and objectives in your State and/or Urban Area Homeland Security Strategy Supported by this Investment. (1,500 char. max)

Nevada Statewide Cyber Assessment and Continuous Monitoring

State Homeland Security Strategy
Critical Infrastructure – Identification, cataloging and protection of all Department of Homeland Security identified sectors of Critical Infrastructure, including Cyber security.
Fusion Center Capabilities
Goal: Enhance measures to secure and harden critical infrastructure targets. (Prevention & Protection)
Objective: Organization.
In close collaboration with public and private sector entities, identify security vulnerabilities pertaining to all potential targets to include, but not limited to: Cyber terrorism, communications systems, utilities, government facilities, transit systems, tourism – resort hotel-casino industry, defense industrial base, etc. on an ongoing basis and upload the results of such assessments to the critical asset management system. Ongoing - Not date specific.

Access Control for Cyber Information
NIMS/Credentialing, Fusion Center capabilities
Goal: Develop, review, update and/or finalize state and local emergency operations plans, continuity of government plans, continuity of operations
plans and terrorism annexes. (Response & Recovery)
Objective: Organization.
Ensure that the relative components of the National Incident Management System (NIMS) and National Response Framework (NRF) are appropriately referenced and/or included in all state, local and tribal emergency operations plans, training, and exercises.

II.B. - Existing capability levels

Describe existing capability levels that address the identified goals/objectives and what will be in place to support the investment prior to the use of FY 2011 funds. (1,500 char. max)

Nevada Statewide Cyber Assessment and Continuous Monitoring
Capabilities in the area addressed by this project are not well formed and are deployed in an inconsistent, ad hoc fashion entity by entity. At this time there is no standardized methodology within the state to measure security vulnerabilities. Capacity that does exist to assess and monitor system vulnerabilities is manual only, resulting in slow response and infrequent assessment. No automated capabilities exist. No other project or effort will result in any advancement prior to use of FFY11 funds and execution of this project.

Access Control for Cyber Information
In discussions with Nevada Cyber Security Committee members throughout the state, no access control systems are known to be in place that are integrated across multiple systems, effective and maintainable. This grant will allow for a complete survey and analysis of the current access control processes to confirm what present aspects are effective, if any, and determine the next steps in developing governance and standards for improved access control and security throughout the state. No other project or effort will result in any advancement prior to use of FFY11 funds and execution of this project.

II.C. - Capability gap(s)

Explain the capability gap(s) that this Investment is intended to address. (1,500 char. max)

Nevada Statewide Cyber Assessment and Continuous Monitoring gaps:
This project will create a standardized approach and software to monitor security vulnerabilities in a continuous manner. This IJ will also fund reports for remediation and training for individuals responsible for addressing vulnerabilities identified by the assessment process.

Access Control for Cyber Information gaps:
Discussions with the Cyber Security Committee members have revealed that there is very little in place in effective, integrated and comprehensive access control processes and systems. Gaps currently exist in governance, standards and systems statewide. This project is intended to specifically identify and address the gaps to create a framework for improved access control leading to improved information security statewide.

Target Capability 1: Critical Infrastructure Protection

III. Project Management - Investment #3

I.C. - Funding Program

Designation	Program	Funding Amount

Primary:	SHSP	$467,500
Secondary:	No Secondary Source	

* **IV.B. - Fusion Center:**

No

If applicable, how much of this Investment will be obligated towards Law Enforcement Terrorism Prevention Activities (LETPA): $0

Target Capability	Amount of Proposed Funding	Percent of Proposed Funding
Critical Infrastructure Protection	$467,500	100%
Total	**$467,500**	**100%**

Solution Area	Amount of Proposed Funding	Percent of Proposed Funding
Planning	$220,000	47.1%
Organization	$60,000	12.8%
Equipment	$127,500	27.3%
Training	$60,000	12.8%
Exercises		
Total	**$467,500**	**100%**

#	Name	Description	Step	Start	End	Funding Amount
1	Nevada Statewide Cyber Assessment and Continuous Monitoring	Implementation of Phase I and II	Execution	01/2012	07/2013	$227,500
2	Access Control for Cyber Information	Implementation of Phase I and II	Execution	01/2012	07/2013	$240,000

V.A - Outcomes to be achieved

Describe the outcomes that will be achieved as a result of this Investment. The outcomes should demonstrate improvement towards building capabilities described in Baseline tab. (1,500 char max)

Nevada Statewide Cyber Assessment and Continuous Monitoring
The goal is for participating entities to quickly recognize and then mitigate cyber security vulnerabilities on an on-going basis. Representatives from volunteer entities will form a pilot group for training on use of monitoring and assessment systems including the design of reporting templates. Project success will be measured by entitles being able to identify critical vulnerability leading to the remediation and reduction of vulnerabilities leading to measureable improvement of the cyber environment and threat characteristic. Sustainment of equipment and training will be assumed by participating entities for their respective individuals and dedicated equipment.

Access Control for Cyber Information
Success of this project will be measured by the recognition of validity and consensus acceptance of the gap analysis, recommendations for standardization and improvement of access control and acceptance of the project plan for implementation by governmental entities.

National Priority 1: Expand Regional Collaboration
National Priority 2: Implement the NIPP

Investment #3

Investment Information - Investment #3

Investment Name: Cyber Security - Critical Infrastructure

Investment Phase: New

Multi-Applicant Investment: No

I. Overview - Investment #3

I.C. - Funding Program

Designation	Program	Funding Amount
Primary:	UASI	$567,500
Secondary:	No Secondary Source	

*** I.D. - Capabilties Building**

Building new capabilities.

I.E. - Investment description

Provide a description of this Investment, including the planning, organization, equipment, training, and/or exercises that will be involved. (2,500 char. max)

This project establishes a statewide capability to assess and monitor the cyber security environment of governmental computer servers and network devices for security vulnerabilities, characterize threats and produce reports for action. Monitoring will cover the cyber environment common to all state, local tribal and special district governmental entities, In-depth scanning, assessment and reporting will be elective to entities who choose to participate. Those participating will be responsible for deploying their desired implementation. The goal is for participating entities to quickly recognize and then mitigate cyber security vulnerabilities on an on-going basis.
The Nevada Cyber Security Committee NCSC will provide oversight, and a consultant will be procured to will develop a Request For Proposal to evaluate integrated solutions, and develop policies and agreements. Equipment identified by RFP will be procured, including monitoring software and hardware, licensing, and servers for initially participating entities. A contract programmer will customize software for specific installs. Training will address system and report utilization, and installation and maintenance.
This Phase 1 is an effort to develop standards and enhance access control into information technology (IT) systems for state, local, tribal and special district governmental entities. The ultimate goal is to protect cyber-based information and systems operation through highly effective access control. With oversight by the NCSC, a consultant will be procured via RFP process. Consultant will conduct a survey of present policies, procedures and protections, and perform a gap analysis. A report and project plan will be developed that will include recommended standards for access control, prioritized needs of entities relative to the standards, cost estimates, and a governance model to coordinate change control and standards update. Following phases will address implementation of standards and development of trusted relationships. Note that this project will use combined UASI and SHSP funding by design and agreement.
This project will establish a standard and structure for data disaster recovery (DDR) plans state-wide by establishing a pilot DDR plan for Clark County. This part of the project uses UASI funding only. A consultant will be procured to develop the detailed DDR plan used to recover computer systems and associated data in the event of a disaster.

II. Baseline - Investment #3

II.A. - Goals and Objectives

Identify the goals and objectives in your State and/or Urban Area Homeland Security Strategy Supported by this

Investment. (1,500 char. max)

Assessment and Continuous Monitoring:
Goal 2 Strengthen Information Sharing and Collaboration in Las Vegas UA
Objective 2.3 Enhance cyber security detection and response capability among regional partners
Goal 4 Protect and maintain the integrity of regional critical systems and infrastructure
Objective 4.4 Enhance cyber security awareness at 25% of the level one and level two facilities over the next two years
Access Control for Information:
Goal 2 Strengthen Information Sharing and Collaboration in LVUA
Objective 2.2 Enhance information sharing capabilities among regional partners
[specifically by improving info sharing through trusted relationships and efficient, protected access]
Objective 2.3 Enhance cyber security detection and response capability among regional partners
Disaster Recovery Planning:
Goal 1 Implement NIMS and NRF to ensure health and safety of resident, visitors and responders
Objective 1.1 Integrate, update, validate and maintain.[in particular, prepare a government Response Plan per NRF Chapter II, pg 28]
Goal 2 Strengthen Information Sharing and Collaboration in LVUA
Objective 2.2 Enhance information sharing capabilities among regional partners
Objective 2.3 Enhance cyber security detection and response capability among regional partners
Goal 3 Strengthen LVUA plans that ensure public health and safety of residents, visitors and responders
Objective 3.1 Enhance and implement existing local and regional emergency plans biannually

II.B. - Existing capability levels

Describe existing capability levels that address the identified goals/objectives and what will be in place to support the investment prior to the use of FY 2011 funds. (1,500 char. max)

Cyber capabilities are not well formed and are deployed in an inconsistent, ad hoc fashion. Currently there is no standardized methodology within the state to measure security vulnerabilities. Capacity that does exist to assess and monitor system vulnerabilities is manual only, No automated capabilities exist. No other project or effort will result in any advancement prior to use of FFY11 funds and execution of this project.
In discussions with Nevada Cyber Security Committee members throughout the state, no access control systems are know to be in place that are integrated across multiple systems, effective and maintainable. This grant will allow for a complete survey and analysis of the current access control processes to confirm what present aspects are effective, if any, and determine the next steps in developing governance and standards for improved access control and security throughout the state. No other project or effort will result in any advancement prior to use of FFY11 funds and execution of this project.
This project will use the current Business Impact Analysis (BIA) developed by a consultant and updated by Clark County staff to ensure that data and technology resource recovery plans and procedures for critical and essential public safety services are initiated and completed. Some DDR "plans" do exist elsewhere to inconsistent standard, however no comprehensive effort will result in any advancement prior to use of FFY11 funds.

II.C. - Capability gap(s)

Explain the capability gap(s) that this Investment is intended to address. (1,500 char. max)

Nevada Statewide Cyber Assessment and Continuous Monitoring gaps:
This project will create a standardized approach and software to monitor security vulnerabilities in a continuous manner. This IJ will also fund reports for remediation and training for individuals responsible for addressing vulnerabilities identified by the assessment process.

Access Control for Cyber Information gaps:
Discussions with the Cyber Security Committee members have revealed that there is very little in place in effective, integrated and comprehensive access control processes and systems. Gaps currently exist in governance, standards and systems statewide. This project is intended to specifically identify and address the gaps to create a framework for improved access control leading to improved information security statewide.

State-Wide Data Disaster Recovery Planning gaps:
Clark County and the LVUA currently does not have a data disaster recovery plan to recover computer systems and associated data in the event of a natural, malevolent or technical disaster. This project will ensure that data and technology resource recovery plans and procedures for timely and prioritized recovery of critical public safety IT services, as identified in Clark County's BIA are initiated and completed.

Target Capability 1: Critical Infrastructure Protection

III. Project Management - Investment #3

I.C. - Funding Program

Designation	Program	Funding Amount
Primary:	UASI	$567,500
Secondary:	No Secondary Source	

*** IV.B. - Fusion Center:**

No

If applicable, how much of this Investment will be obligated towards Law Enforcement Terrorism Prevention Activities (LETPA): $0

Target Capability	Amount of Proposed Funding	Percent of Proposed Funding
Critical Infrastructure Protection	$567,500	100%
Total	**$567,500**	**100%**

Solution Area	Amount of Proposed Funding	Percent of Proposed Funding
Planning	$340,000	59.9%
Organization	$40,000	7%
Equipment	$127,500	22.5%
Training	$60,000	10.6%
Exercises		
Total	**$567,500**	**100%**

#	Name	Description	Step	Start	End	Funding Amount
1	Nevada Statewide Cyber Assessment and Continuous Monitoring	Implementation of Phase I and II	Execution	01/2012	07/2013	$227,500
2	Access Control for Cyber Information	Implementation of Phase I and II	Execution	01/2012	07/2013	$160,000
3	State-Wide Disaster Recovery Planning (Clark County Pilot Plan)	Implementation of Phase I and II	Planning	01/2012	07/2013	$180,000

V.A - Outcomes to be achieved

Describe the outcomes that will be achieved as a result of this Investment. The outcomes should demonstrate improvement towards building capabilities described in Baseline tab. (1,500 char max)

Nevada Statewide Cyber Assessment and Continuous Monitoring
The goal is for participating entities to quickly recognize and then mitigate cyber security vulnerabilities on an on-going basis. Representatives from volunteer entities will form a pilot group for training on use of monitoring and assessment systems including the design of reporting templates. Project success will be measured by entitles being able to identify critical vulnerability leading to the remediation and reduction of vulnerabilities leading to measureable improvement of the cyber environment and threat characteristic. Sustainment of equipment and training will be assumed by participating entities for their respective individuals and dedicated equipment.

Access Control for Cyber Information
Success of this project will be measured by the recognition of validity and consensus acceptance of the gap analysis, recommendations for standardization and improvement of access control and acceptance of the project plan for implementation by governmental entities.

State-Wide Data Disaster Recovery Planning
The goal of this project will be a pilot project which will be conducted during a 12 month window of time and will develop a data disaster recovery plan for critical IT services supporting public safety in the LVUA. The target metric is Return to Operations (RTOs) of 72 hours or less

National Priority 1: Expand Regional Collaboration
National Priority 2: Implement the NIPP