**To:** Bay Area UASI Approval Authority

**From:** Catherine Spaulding, Assistant General Manager

**Date:** August 8, 2013

**Re:** Item #5: Cyber, Recovery, and Citizen Preparedness

## Recommendation:

Approve the proposed allocation of $776,700 of FY13 UASI funds:

- $405,220 – Three cyber security analyst positions in the NCRIC
- $254,480 – Recovery planning and preparations
- $117,000 – Bay72 regional expansion

## Attachments:

Appendix A: Proposal for Utilization of Funds, NCRIC Cyber Program
Appendix B: NCRIC Cyber Org Chart
Appendix C: Bay Area Recovery Planning Survey

## Discussion:

### *Background*

At the June 13th Approval Authority Meeting, the Management Team announced the availability of $817,000 from the FY13 UASI allocation. These funds became available when we learned that the State was planning to retain 17% of the total grant allocation rather than 20%. The actual amount available for reallocation is $776,700 once the M&A amount is extracted.

At the June meeting, the Management Team recommended that the Approval Authority allocate these funds to cyber security, recovery, and citizen preparedness. The Management Team made this recommendation because these are critical gaps that have been identified through our risk management program, that have been identified by FEMA as being critical priorities, and that have hitherto not received significant funding in our region. The Approval Authority requested that the Management Team provide specific details in the August meeting on how these funds – particularly the cyber funds – would be spent.

### *Cyber Security*

In May this year, the NCRIC established a Cyber Unit to collect and share cyber information as well as provide intelligence analysis and defense. The Unit consists of five FTEs and implements four initiatives: Cyber Outreach, Cyber Incident Reporting, Cyber Liaison Officers, and Automated Threat Information Collection System. Please see page 9 of Attachment A "Proposal for Utilization of Funds, NCRIC Cyber Program" for more information on these programs. Please also see Appendix B for the NCRIC Cyber Program Organization Chart.

The Cyber Unit has been funded on a pilot basis through October 2013 by the Department of Homeland Security via the White House. The Management Team recommends allocating $405,220 from FY13 UASI funds to support three of the five Cyber Unit positions for a twelve month period.

### *Recovery Planning and Preparations*

At the March 2013 Approval Authority meeting, the body discussed the need and importance of future regional work on recovery. Regional Program Manager Janell Myhre has since surveyed all 12 counties and three major cities concerning work completed to date in the areas of outside agency stakeholder discussions, emergency pre-planning, and plans (see Appendix C: Bay Area Recovery Planning Survey). Regional Program Manager Janell Myhre has also discussed with multiple stakeholders their priorities for regional work in the recovery area.

The Management Team recommends allocating $254,480 that will be used to pay for staff and/or consultant time to conduct the following work:

- Gain pre-approval from FEMA for the region's debris management plans so that regional operational areas could increase their reimbursement rate from FEMA from 75% to 80%.
- Assist those OAs and Core Cities who have not yet developed preparations for permitting waivers to do so, based on work already developed in the region.
- Assist those OAs and Core Cities who have not yet developed continuity of operations and continuity of government plans to do so, based on work already developed in the region.
- Work with region's Core Cites to develop/support development of a Disaster Recovery Framework and Recovery Support Functions, based on FEMA's national model, which includes planning around economic recovery, health and social services, housing, infrastructure, and natural and cultural resources. This framework could be used as a model for other cities and OAs in the bay area region.

These tasks would be confirmed and prioritized through further stakeholder consultations and a sub-committee on Recovery established as part of the RCPT workgroup.

***Bay72 Regional Expansion***

Bay72 (previously called the SF72 project) creates engaging and dynamic online homes for citizen preparedness as well as local coordination sites for when disaster strikes. To date the project has been developed for San Francisco with the intention of serving as a pilot for the region. All of the code for this site is open source, so it will be low cost and easy to replicate regionally.

In March 2013, the Approval Authority approved $200,000 of regional funds (FY11 and FY12 salary savings) to support the Bay72 project. These funds will support the completion of the design and build out of the SF72 website, including citizen feedback.

The Management Team recommends allocating an additional $117,000 from FY13 UASI funds to Bay72 to help the two other Major Cities (Oakland and San Jose) as well as one North Bay Operational Area to begin to develop their own locally-tailored sites (e.g., “Oak72” and “SJ72”). The funds will support a series of workshops so that these local jurisdictions can develop their own local messages and content, printed materials, and other collateral content.

# 080813

# AGENDA ITEM # 5

# APPENDIX A

## PROPOSAL FOR UTILIZATION OF FUNDS, NCRIC CYBER PROGRAM

# Proposal for Utilization of Funds

# NCRIC CYBER PROGRAM

## Northern California Regional Intelligence Center

# NCRIC Cyber Program
# Utilization of Funds

I. BACKGROUND

II. SCOPE

III. NCRIC CYBER UNIT STAFFING

a. CYBER PROGRAM LEAD ANALYST

b. STRATEGIC CYBER INTELLIGENCE ANALYST

c. TACTICAL CYBER INTELLIGENCE ANALYST

d. CYBER SECURITY SPECIALIST

e. CYBER OUTREACH COORDINATOR

IV. DESCRIPTION OF NCRIC CYBER PROGRAM INITIATIVES

a. CYBER OUTREACH PROGRAM (COP)

b. CYBER INCIDENT REPORTING (CIR) PROGRAM

c. CYBER LIAISON OFFICERS (CLO) PROGRAM

d. AUTOMATED THREAT INFORMATION COLLECTION SYSTEM (ATICS)

e. CYBER VULNERABILITY ASSESSMENT PROGRAM (CVAP)

V. APPENDIX A: SAMPLE CYBER INCIDENT RESPONSE (CIR) RUBRIC

# NCRIC CYBER PROGRAM
# UTILIZATION OF FUNDS

## I. BACKGROUND

The NCRIC established its cyber program in 2011, focusing initially on providing NCRIC partners with strategic and regional cyber threat analytical products. The NCRIC cyber program has grown since then, resulting in collaborative training efforts with the U.S. Secret Service and DHS, the creation of the Cyber Intelligence Network, the creation and dissemination of joint intelligence bulletins with FBI analysts, public sector and private sector cyber outreach, and recognition of the NCRIC's cyber capabilities amongst Fusion Centers, law enforcement, and the Federal cyber security community.

The purpose of this document is to guide the utilization of funding to further expand the NCRIC cyber program.

## II. SCOPE

The scope of this document is to describe in detail the NCRIC's plans to utilize funding sources to expand the NCRIC's cyber capabilities.

## III. NCRIC CYBER UNIT STAFFING

The NCRIC plans on expanding and increasing its capabilities to meet four major needs within the NCRIC area of responsibility: (1) *Cyber Information Collection*, (2) *Cyber Defense*, (3) *Cyber Information Sharing*, and (4) *Cyber Intelligence Analysis*.

With these needs in mind, the NCRIC intends to staff the cyber unit with:

a. One **Cyber Program Lead Analyst** focused on managing and developing programs for NCRIC partners and the National Fusion Center Association, coordinating between the different cyber program components, as well as liaising with NCRIC internal-initiatives and external agencies.

b. One **Strategic Cyber Intelligence Analyst** focused on strategic analysis and assessment of cyber threats to the region, with a strong understanding of cyber threat trends and intelligence reporting standards.

c. One **Tactical Cyber Intelligence Analyst** focused on tactical and technical threat analysis and investigative threat support, with experience in computer forensics and incident response.

d. One **Cyber Security Specialist** and penetration tester experienced with vulnerability assessments, network and system defense, and advanced information technology solutions (including managing honeypots and deploying intrusion detection systems).

e. One **Cyber Outreach Coordinator** focused on cyber outreach, developing and managing training, working with NCRIC Partners within the region on State and local cyber efforts, and developing websites and other interactive web-based programs for the cyber program.

Each position will support the others, as it is expected there will be overlap in duties, necessitating strong coordination between the specialists.

## CYBER LEAD ANALYST

The Cyber Program Lead Analyst will be responsible for assisting with the development of new cyber security initiatives within the NCRIC and ensuring the specialists and Fusion Center have the support necessary to guarantee their success.

The Cyber Program Lead Analyst will assist the specialists in navigating and building the relationships necessary to promote and develop new projects, as well as manage current cyber initiatives in progress.

As such, it is expected the Cyber Program Lead Analyst will have experience working with partners within the Fusion Center community, the Federal cyber security and intelligence realms, as well as internal NCRIC components. The Cyber Program Lead Analyst will also liaise with agencies and represent the NCRIC in the national conversation about cyber security, and ensure all programs developed meet the need of NCRIC partners.

The Cyber Program Lead Analyst will work closely with all of the specialists in the NCRIC Cyber Unit.

Regarding chain of command, the Cyber Lead Analyst will report to the NCRIC Homeland Security Program Lead Analyst to ensure all efforts are in line with the NCRIC's overall goals and mission.

**Minimum Requirements for position:**

- Experience developing and managing cyber security and intelligence projects.
- Strong understanding of current national, state and local cyber resources, efforts, and participating agencies.
- Strong oral and written communications skills.
- Experience with initiative proposals and management.
- Experience and/or training with/in all aspects of cyber security and intelligence, including forensics, analysis, and network defense.
- Strong understanding of intelligence reporting standards.

**Examples of deliverables expected from the Cyber Lead Analyst:**

- Regular progress reports on all current and future cyber initiatives.
  - Cyber Incident Reporting Process
  - Cyber Outreach Program
  - Automated Threat Information Collection System (ATICS)
  - Cyber Vulnerability Assessment Program (CVAP)
- Written proposals for new cyber initiatives.
- Briefings on NCRIC cyber efforts.

## STRATEGIC CYBER INTELLIGENCE ANALYST

The Strategic Cyber Intelligence Analyst will be responsible for monitoring, increasing awareness about, and developing intelligence on threats to the NCRIC AOR. This will include creating and managing the cyber threat monitor update, updating a cyber threat blog on the NCRIC website, and developing analytical intelligence products on threat actors and major incidents of note.

The Strategic Cyber Intelligence Analyst will also create and update specific intelligence products on the threats to the NCRIC AOR detailed in the overall NCRIC Threat Assessment, including the Chinese Hacker Threat, the Hacktivist Threat, Eastern-European Cyber Criminal Organizations, Collateral Damage from Super Cyber Weapons, and Cyber Terrorists. This will be in addition to monitoring and producing products on cyber trends and new tactics, techniques and procedures (TTPs) used by cyber threat actors.

It is expected the Strategic Cyber Analyst will be capable of briefing NCRIC partners on all strategic analysis products and efforts on a regular basis. As such, the Strategic Cyber Analyst will work closely with the Cyber Outreach Coordinator to ensure partners receive intelligence products, and are satisfied their needs are being met. Presentations by the Strategic Cyber Analyst will be coordinated through the Cyber Outreach Coordinator.

The Strategic Cyber Analyst will also work with the Tactical Cyber Analyst on joint products, as well as to respond to cyber incidents and reporting received by the NCRIC.

**Minimum Requirements for position:**

- Strong oral and written communications skills.
- Experience in producing intelligence products focused in the cyber field.
- A strong understanding of the cyber threat.
- Experience in working with other agencies to develop intelligence.
- Strong understanding of intelligence reporting standards.

**Examples of deliverables expected from the Strategic Cyber Intelligence Analyst:**

- Formal documentation and description of the Cyber Incident Reporting (CIR) intake and response model
- Cyber Threat Monitor Updates on a month to two-month rotation
- Regular updates to the NCRIC cyber threat blog
- Intelligence Products on all cyber threats to the NCRIC AOR
- Intelligence Products on all cyber threat trends
- Intelligence Products on all new cyber techniques, tactics and procedures used by threat actors

## TACTICAL CYBER INTELLIGENCE ANALYST

The Tactical Cyber Intelligence Analyst will be responsible for responding to incidents within the NCRIC AOR that require basic technical support. This will include triage, and taking at least the first steps to assist NCRIC Partners respond to intrusions and attacks.

The Tactical Cyber Intelligence Analyst will help investigators understand technical case data, whether raw investigative data or the output from technical response partners, whether private or public (e.g. RCFLs). The overall goal of the Tactical Cyber Intelligence Analyst will be to assist NCRIC Partners increase their ability to respond to threats, cyber incidents brought to them by constituents, and attacks on their own networks.

At least quarterly, the Tactical Cyber Intelligence Analyst will brief NCRIC Partners on new TTPs used by cyber threat actors.

The Tactical Cyber Intelligence Analyst will work closely with the Strategic Cyber Threat Intelligence Analyst as well as the Cyber Security Specialist on cyber threat incident response and reporting. Further, in coordination with the Cyber Security Specialist, the Tactical Cyber Intelligence Analyst will manage the Automated Threat Information Collection System (see below program descriptions).

The Tactical Cyber Intelligence will be involved in advising on and assisting with the deployment and management of advanced information technology defense solutions, in support of the NCRIC Information Technology unit and the Cyber Security Specialist.

**Minimum Requirements for position:**

- This position is intended for a cyber investigator or a computer forensics specialist.
- Strong oral and written communications skills.
- Experience in computer forensics.
- Experience in incident response and triage.
- Experience in law enforcement cyber investigations.

**Examples of deliverables expected from the Tactical Cyber Intelligence Analyst:**

- Incident response and after action reports.
- Technical Intelligence Products and briefings
- Clear documentation of NCRIC internal standards and processes for cyber incidents.
- Development and management of the Automated Threat Information Collection System

## CYBER SECURITY SPECIALIST

The Cyber Security Specialist will manage the NCRIC Cyber Vulnerability Assessment Program (CVAP) in coordination with the NCRIC Infrastructure Protection (IP) Unit (see below). This will include working with NCRIC Partners on network defense, target hardening, and conducting authorized penetration testing, as requested by NCRIC partners.

The Cyber Security Specialist will also be the lead on managing the Automated Threat Information Collection System, sùpported by the Technical Cyber Intelligence Analyst.

In coordination with the NCRIC information Technology team, the Cyber Security Specialist will help develop and deploy advanced information technology defense solutions, including honeypots, malware analysis tools, and intrusion detection systems.

It will be expected that the Cyber Security Specialist will develop and maintain a strong working relationship with investigatory bodies involved in cyber incident response and investigations, including local REACT Task Forces, the FBI Cyber Units, and RCFLs.

**Minimum Requirements for position:**

- This position is intended for a computer engineer, programmer, or computer science applicant.
- Extensive experience in computer forensics.
- Extensive experience in Penetration Testing.
- Proficiency in the use of industry-recognized cyber-security tools and techniques
- Experience with law enforcement cyber investigations
- Proficiency in the deployment of advanced information technology defense solutions

**Examples of deliverables expected from the Cyber Security Specialist:**

- Documentation on and development of the cyber vulnerability assessment program (CVAP), including the scope, performance requirements, project plan and program Standard Operating Procedures.
- Development and management of the ATICS program
- A formal document clearly explaining the model used by ATICS to take-in IOC's and malicious IP addresses and produce machine-readable reports for consumption,
- A clear explanation of the process to join the ATICS program and its benefits.

## CYBER OUTREACH PROGRAM COORDINATOR

The Cyber Outreach Coordinator will work closely with the NCRIC Private Sector Outreach Manager to develop and manage the Cyber Outreach Program (COP) for NCRIC partners.

COP includes the development and management of training program to enhance the cyber incident response and cyber investigation capabilities of NCRIC partners, as well as to help partners understand how to report cyber incidents to the NCRIC and the larger cyber security community. Similar to the current Terrorism Liaison Officer TLO program, "Cyber Liaison Officers" (CLO's) will be trained in identifying and reporting cyber incidents and managing cyber investigations.

Some examples of courses to be developed by the Cyber Outreach Coordinator include "Cyber Security Essentials for Law Enforcement", "The Importance of SCADA System Defense", "Cyber Investigators Training Level One", "Prosecuting Cyber Crime", etc.

The Cyber Outreach Coordinator will also manage a COP Cyber Working Group, conferences, and the production of cyber products relevant to the Fusion Center partner community. One such cyber-specific product will include a weekly Cyber Partner Update ("Cyber-PUB"). The Cyber-PUB will summarize all relevant cyber information from the day to keep partners apprised of all relevant cyber reporting and products flowing to the participating Fusion Center.

Separate from the Cyber-PUB the Cyber Outreach Coordinator will develop and disseminate Best Practices products for NCRIC partners, with such topics as "How To Protect Yourself from Spear Phishing" and "Resources For Protecting Yourself from a DDoS attack".

The Cyber Outreach Coordinator will also be expected to assist in managing the Cyber Intelligence Network portal, and will need strong website development skills to develop new web-based programs and tools for the Cyber Unit.

The Cyber Outreach Coordinator will work closely with the NCRIC Private Sector Outreach Manager as well as the entire NCRIC Cyber Unit on products and training to ensure it is accurate and effective. Each member of the NCRIC Cyber Unit will be expected to provide training within their areas of expertise and responsibility.

**Minimum Requirements for position:**

- Extremely strong oral and written communications skills.
- Experience in cyber investigations and response.
- Proficiency in Web design
- Strong relationships with the Law Enforcement Community and Cyber Security Communities

**Examples of deliverables expected from the Cyber Outreach Coordinator:**

- Detailed documentation and description of the Cyber Outreach Program (COP)
- Detailed documentation and description of the Cyber Liaison Officer (CLO) Program
- Course curriculums, class brochures and materials
- Marketing materials for COP
- CLO training programs' expected outcomes
- Regular COP assessments and reports
- CIN Website Updates
- Web-based tools and initiatives for COP
- Producing the weekly (LES) and (FOUO) Cyber PUBs
- A formal document clearly explaining the CIN model, reporting, and membership vetting process

## VI. DESCRIPTION OF NCRIC CYBER PROGRAM INITIATIVES

The following will describe the programs mentioned above and will be developed and managed by the NCRIC Cyber Unit.

### a. Cyber Outreach Program (COP)

The goal of the Cyber Outreach Program will be to promote cyber incident reporting amongst Fusion Center partners, as well as to increase their capabilities in regards to cyber incident response and investigations.

COP will include the Cyber Incident Reporting program, as well as the Cyber Liaison Officers Program.

### b. Cyber Incident Reporting (CIR) Program

Appendix A includes a sample Cyber Incident Response rubric to be used by cyber threat intelligence analysts to intake, prioritize, and respond to cyber suspicious activity reporting quickly and methodically. This standardized approach to CIR categorization and prioritization will assist in the identification of dangerous cybercrime campaigns, botnets, malware and other threats by ensuring indicators of their existence receive the attention necessary to respond appropriately and quickly.

The ultimate goal is to utilize the rubric in a standardized CIR intake process, through which CIRs can be received, categorized, prioritized, escalated if necessary, responded to by the appropriate parties, and stored in a nationally accessible database for information sharing purposes and trend analysis.

### c. Cyber Liaison Officers (CLO) Program

Just as the Terrorism Liaison Officers (TLO) Program trains partners on how to report Suspicious Activity and identify the indicators of terrorism, the CLO program will train partners on reporting cyber incidents, as well as how to respond to and investigate cyber incidents when brought to them by constituents.

### d. Automated Threat Information Collection System (ATICS)

The NCRIC will develop a system for automatically collecting and disseminating malicious IP addresses and other indicators of compromise (IOC's)[1] in real-time and in a *standardized* machine-readable format. This Automated Threat Information Collection System ("ATICS") model will leverage and be informed by all other similar programs currently operating or in development, including LA-SAFE's blacklist program and the Mitre STIX/TAXII program.

The ATICS model will allow for a variety of data sources, including firewalls, honeypots, sensors, and intrusion detections systems ("IDS"), as well as data streams from partner systems that will (1) receive the threat indicators and malicious IP addresses from ATICS, but also (2) feed into ATICS, making the system more reliable and resilient. The ATICS model will include an automated internal review process to ensure false-positives are minimized.

[1] As defined by RSA, an *Indicator of Compromise* (IOC) is a forensic artifact or remnant of an intrusion that can be identified on a host or network. blogs.rsa.com/understanding-indicators-of-compromise-ioc-part-i

# Cyber Incident Reporting (CIR) Rubric

**IMMEDIATE RESPONSE NECESSARY**

Cyber incident involving malicious activity consistent with indicators of an intrusion/compromise that poses a significant threat to the victim or community and requires immediate response and remediation. Examples include the discovery of harmful zero-day exploits, an extensive cybercrime campaign, or a new type of malware.

**ACTIONABLE**

Unusual activity or behavior consistent with indicators of an intrusion/compromise that lacks a legitimate explanation or appears to be unknown malware and/or a new cybercrime tactic, technique, or procedure, which does not require an immediate response. Examples include the discovery of potential zero-day exploits, insider threats, targeted spearphishing campaigns, and indicators of a new botnet.

**ROUTINE**

Observed activity consistent with known malware and/or cybercrime tactics, techniques and procedures (TTPs) that pose little threat to the victim and greater community. Examples include known malware infections requiring simple remediation measures, surreptitious software add-ons (e.g. browser buttons), or rudimentary spam campaigns.

**POTENTIAL**

Indicators of an intrusion/compromise that could also be associated with abnormal behavior or activity, including user-error, software/hardware malfunction, etc. Further investigation required to make final determination.

**NO THREAT**

No threat is involved in the incident and there are no indicators of compromise or other malicious activity. Examples include incidents that are the result of software or hardware malfunctions, user-error, or normal (but unexpected) processes.

### Purpose of the CIR Rubric

The purpose of this rubric is to help cyber threat intelligence analysts intake, prioritize, and respond to cyber suspicious activity reporting quickly and methodically. This standardized approach to CIR categorization and prioritization will assist in the identification of dangerous cybercrime campaigns, botnets, malware and other threats by ensuring indicators of their existence receive the attention necessary to respond appropriately and quickly.

The ultimate goal is to utilize this rubric in a standardized CIR intake process, through which CIRs can be received, categorized, prioritized, escalated if necessary, responded to by the appropriate parties, and stored in a nationally accessible database for information sharing purposes and trend analysis.

# 080813

# AGENDA ITEM # 5

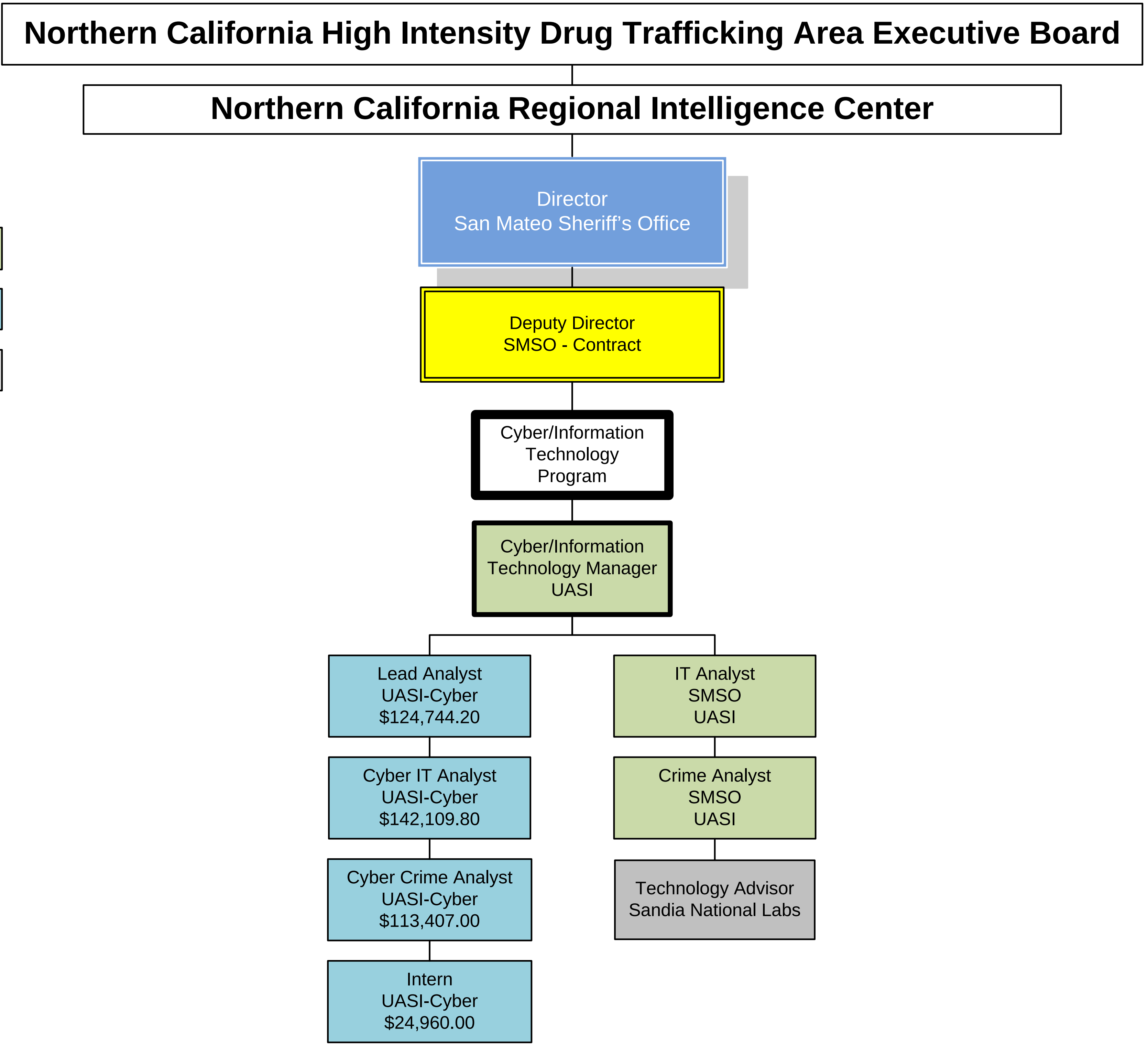
# APPENDIX B

## NCRIC CYBER ORGANIZATIONAL CHART

(3) Staff UASI Funded

(4) Requested UASI Funded Cyber/IT Personnel $405,221

(1) Agency Funded Part-Time Personnel



Northern California High Intensity Drug Trafficking Area Executive Board

Northern California Regional Intelligence Center

Director
San Mateo Sheriff's Office

Deputy Director
SMSO - Contract

Cyber/Information
Technology
Program

Cyber/Information
Technology Manager
UASI

Lead Analyst
UASI-Cyber
$124,744.20

Cyber IT Analyst
UASI-Cyber
$142,109.80

Cyber Crime Analyst
UASI-Cyber
$113,407.00

Intern
UASI-Cyber
$24,960.00

IT Analyst
SMSO
UASI

Crime Analyst
SMSO
UASI

Technology Advisor
Sandia National Labs

Updated on: 7/25/2013

# 080813

# AGENDA ITEM # 5

# APPENDIX C

## BAY AREA RECOVERY PLANNING SURVEY

# Bay Area Recovery planning survey _ July 2013

| Jurisdiction Name | Outside agency engagement | | | | Emergency waivers | | | | Plans | | | | | Summary by Jurisdiction | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Public private partner | Utilities planning | Water systems planning | Communications planning (Verizon, Comcast, PacBell, etc) | Land use | City/county permitting | Emergency procurement policies | Point of Distribution mapping | Continuity of Operations (COOP) | Continuity of government (COG) | Critical Lifelines planning | Local Hazard Mitigation Plan | Long Term Housing | **Y** | **N** | **WIP** |
| Alameda | Y | Y | Y | Y | Y | Y | Y | WIP | Y | Y | WIP | WIP | N | 9 | 1 | 3 |
| Contra Costa | WIP | N | N | WIP | Y | Y | Y | Y | WIP | Y | WIP | Y | WIP | 6 | 2 | 5 |
| Marin | N | WIP | N | N | N | N | N | WIP | Y | Y | N | WIP | N | 2 | 8 | 3 |
| Napa | Y | Y | Y | Y | Y | WIP | Y | WIP | WIP | WIP | WIP | WIP | WIP | 6 | 0 | 7 |
| Solano | Y | Y | Y | Y | WIP | N | WIP | Y | Y | Y | Y | Y | WIP | 9 | 1 | 3 |
| Sonoma | N | Y | WIP | N | WIP | Y | Y | WIP | Y | Y | WIP | Y | N | 6 | 3 | 4 |
| San Mateo | WIP | WIP | WIP | WIP | N | N | Y | WIP | N | Y | N | Y | N | 3 | 5 | 5 |
| San Francisco | Y | Y | Y | Y | Y | N | Y | WIP | WIP | Y | WIP | Y | WIP | 8 | 1 | 4 |
| Santa Clara | N | N | WIP | N | N | N | N | WIP | WIP | N | N | Y | N | 1 | 9 | 3 |
| Santa Cruz | WIP | WIP | WIP | Y | WIP | WIP | Y | WIP | WIP | WIP | WIP | Y | WIP | 3 | 0 | 10 |
| San Benito | Y | Y | Y | WIP | N | N | Y | WIP | Y | WIP | Y | WIP | WIP | 6 | 2 | 5 |
| Monterey | y | WIP | Y | Y | WIP | N | WIP | WIP | WIP | WIP | Y | WIP | N | 4 | 2 | 7 |
| San Jose | Y | N | Y | N | N | N | WIP | Y | Y | Y | N | Y | N | 6 | 6 | 1 |
| Oakland | Y<br>beginning stages | Y<br>beginning stages | Y<br>beginning stages | N | N | N | WIP | WIP | Y | Y | N | Y | N | 6 | 5 | 2 |
| Region/ State | Y | WIP | WIP | Y | Y | Y | Y | N | Y | Y | WIP | N/A | WIP | 7 | 1 | 4 |
| **Summary** | **9Y<br>3N<br>3WIP** | **7Y<br>3N<br>5WIP** | **8Y<br>2N<br>5WIP** | **7Y<br>5N<br>3WIP** | **5Y<br>6N<br>4WIP** | **4Y<br>9N<br>2WIP** | **9Y<br>2N<br>4WIP** | **3Y<br>1N<br>11WIP** | **8Y<br>1N<br>6WIP** | **10Y<br>1N<br>4WIP** | **3Y<br>5N<br>7WIP** | **9Y<br>0N<br>5WIP** | **0Y<br>8N<br>7WIP** | **82Y** | **46N** | **66WIP** |

**Comment LEGEND**

| | |
|---|---|
| Y: | yes |
| N: | no |
| WIP: | work in progress |

Misc comments:
Copies of plans and research included by Marin County, City/County of San Francisco, Napa County
Additional information: Sonoma County has done Staging Area mapping, CalOES Coastal Region is supported by CalOES State operations during the recovery phase.