AGENDA

LOS ANGELES REGIONAL
INTEROPERABLE COMMUNICATIONS SYSTEM AUTHORITY

JOINT OPERATIONS & TECHNICAL COMMITTEE MEETING

Tuesday, September 25, 2018 • 1:30 p.m.
LA-RICS Headquarters – Large Conference Room
2525 Corporate Place, Suite 200, Monterey Park, CA 91754

Los Angeles Regional Interoperable Communications System Authority (the "Authority")

AGENDA POSTED: September 21, 2018

Complete agendas are made available for review at the designated meeting location. Supporting documentation is available at the LA-RICS Office located at 2525 Corporate Place, Suite 200, Monterey Park, CA 91754 during normal business hours and may also be accessible on the Authority's website at http://www.la-rics.org.

OPERATIONS COMMITTEE

Members:

1. **John Geiger**, Los Angeles County, CEO
2. **Kyle Zuniga**, **Chair**, County of Los Angeles Fire Dept.
3. **Tab Rhodes, Vice-Chair**, L.A. County Sheriff's Dept.
4. **Cathy Chidester**, Los Angeles County DHS
5. **Chris Donovan**, Los Angeles Area Fire Chiefs Association
6. **Anthony Vairo**, L.A. County Police Chiefs Association
7. **Elliot Kase**, Alhambra Police Dept.
8. **John Curley**, Covina Police Dept.
9. **Jeff Steinhoff**, Inglewood Police Dept.
10. **Ron Sagmit**, Signal Hill Police Dept.

Alternates:

Mike Iwanaga, Los Angeles County, CEO
Chris Bundesen, County of Los Angeles Fire Dept**.**
Sven Crongeyer, L.A. County Sheriff's Dept.
Karolyn Fruhwirth, Los Angeles County DHS
Eric Zanteson, Los Angeles Area Fire Chiefs Association
Shelly Vander Veen, L.A. County Police Chiefs Association
Vacant, pending
Ric Walczak, Covina Police Dept.
Cardell Hurt, Inglewood Police Dept.
Brian Leyn, Signal Hill Police Dept.

TECHNICAL COMMITTEE

Members:

1. **John Geiger**, Los Angeles County, CEO
2. **Scott England**, **Vice-Chair**, County of Los Angeles Fire Dept.
3. **Tab Rhodes**, Los Angeles County Sheriff's Dept.
4. **Jeffrey Morgan**, Los Angeles County DHS
5. **James Craig**, Manhattan Beach Fire Dept.
6. **Ted Pao**, **Chair**, Los Angeles County Internal Services Dept.
7. **Elliot Kase,** Alhambra Police Dept.
8. **John Curley**, Covina Police Dept.
9. **Jeff Steinhoff**, Inglewood Police Dept.
10. **Ron Sagmit**, Signal Hill Police Dept.

Alternates:

Mike Iwanaga, Los Angeles County, CEO
Rufino Fernandez, County of Los Angeles Fire Dept.
Sven Crongeyer, Los Angeles County Sheriff's Dept.
Kim Buard, Los Angeles County DHS
Eric Zanteson, Los Angeles Area Fire Chiefs Association
Mike Dunning, Los Angeles County Internal Services Dept.
Vacant, pending
Ric Walczak, Covina Police Dept.
Cardell Hurt, Inglewood Police Dept.
Brian Leyn, Signal Hill Police Dept.

Officers:

Scott D. Edson, Executive Director
Joann Huerta, Committees Secretary

NOTE: ACTION MAY BE TAKEN ON ANY ITEM IDENTIFIED ON THE AGENDA

I.   CALL TO ORDER

II.   ANNOUNCE QUORUM – Roll Call

III.   APPROVAL OF MINUTES

    A.   July 24, 2018 – Regular Meeting Minutes

IV.   PUBLIC COMMENTS

V.   CONSENT CALENDAR – (None)

VI.   REPORTS (B-C)

    B.   Status Report Update for LTE

    C.   Status Report Update for LMR

VII.   DISCUSSION ITEMS (D)

Fleet Mapping Status

Agenda Item D

VIII.   ADMINISTRATIVE MATTER (E)

    E.   APPROVE RECOMMENDATION TO THE LA-RICS JOINT POWERS AUTHORITY BOARD OF DIRECTORS TO APPROVE THE LA-RICS' SECURITY POLICIES (POLICY NOS. 027-2018 AND 028-2018)

It is recommended the Joint Operations and Technical Committees:

Approve a recommendation to the Board to adopt the following LA-RICS security policies to enhance the Authority's Information Technology (IT) Security Program:

▪ Board Policy No. 027-2018 – LA-RICS Information Technology Physical Security Policy (Enclosure 1)

- Board Policy No. 028-2018 – LA-RICS Information Technology Risk Assessment and Audit Compliance Policy (Enclosure 2)

Agenda Item E

IX.   MISCELLANEOUS – NONE

X.   ITEMS FOR FUTURE DISCUSSION AND/OR ACTION BY THE COMMITTEE

XI.   CLOSED SESSION REPORT - NONE

XII.   ADJOURNMENT AND NEXT MEETING:

Tuesday, November 27, 2018, at 1:30 p.m., location forthcoming.

COMMITTEE MEETING INFORMATION

Members of the public are invited to address the LA-RICS Committee on any item on the agenda prior to action by the Committee on that specific item. Members of the public may also address the Committee on any matter within the subject matter jurisdiction of the Committee. The Committee will entertain such comments during the Public Comment period. Public Comment will be limited to three (3) minutes per individual for each item addressed, unless there are more than ten (10) comment cards for each item, in which case the Public Comment will be limited to one (1) minute per individual. The aforementioned limitation may be waived by the Committee's Chair.

(NOTE: Pursuant to Government Code Section 54954.3(b) the legislative body of a local agency may adopt reasonable regulations, including, but not limited to, regulations limiting the total amount of time allocated for public testimony on particular issues and for each individual speaker.)

Members of the public who wish to address the Committee are urged to complete a Speaker Card and submit it to the Committee Secretary prior to commencement of the public meeting. The cards are available in the meeting room. However, should a member of the public feel the need to address a matter while the meeting is in progress, a card may be submitted to the Committee Secretary prior to final consideration of the matter.

It is requested that individuals who require the services of a translator contact the Committee Secretary no later than the day preceding the meeting. Whenever possible, a translator will be provided. Sign language interpreters, assistive listening devices, or other auxiliary aids and/or services may be provided upon request. To ensure availability, you are advised to make your request at least 72 hours prior to the meeting you wish to attend. (323) 881-8291 or (323) 881-8295

SI REQUIERE SERVICIOS DE TRADUCCION, FAVOR DE NOTIFICAR LA OFICINA CON 72 HORAS POR ANTICIPADO.

The meeting is recorded, and the recording is kept for 30 days.

JOINT OPERATIONS & TECHNICAL COMMITTEE MEETING MINUTES

LOS ANGELES REGIONAL INTEROPERABLE COMMUNICATIONS SYSTEM AUTHORITY

Tuesday, July 24, 2018 · 1:30 p.m.
LA-RICS Headquarters – Large Conference Room
2525 Corporate Place, Suite 200, Monterey Park, CA 91754

Operations Committee Members Present:
Mike Iwanaga, Los Angeles County, CEO
Kyle Zuniga, Chair, County of Los Angeles, Fire Department
Tab Rhodes, Vice-Chair, Lieutenant, Los Angeles County Sheriff's Department
Cathy Chidester, Los Angeles County DHS
Ric Walczak, Lieutenant, Covina Police Department
Brian Leyn, Captain, Signal Hill Police Department

Technical Committee Members Present:
Mike Iwanaga, Los Angeles County, CEO
Scott England, Vice-Chair, Telecommunications Engineer Command and Control, LACoFD
Information Officer, EMS Agency, County of LADHS
Tab Rhodes, Lieutenant, Los Angeles County Sheriff's Department
Kim Buard, Los Angeles County DHS
Ted Pao, Chair, Information Technology Specialist, Los Angeles County Internal Services Department
Ric Walczak, Lieutenant, Covina Police Department
Brian Leyn, Captain, Signal Hill Police Department

Absent:
John Geiger, Los Angeles County, CEO
Chris Donovan, Los Angeles Area Fire Chiefs Association
Jeffrey Morgan, Los Angeles County DHS
James Craig, Manhattan Beach Fire Department
Anthony Vairo, L.A. County Police Chiefs Association
Elliot Kase, Assistant Chief of Police, Alhambra Police Department
John Curley, Chief of Police, Covina Police Department
Jeff Steinhoff, Sergeant, Inglewood Police Department
Ron Sagmit, Lieutenant, Signal Hill Police Department

Officers Present:
Scott D. Edson, LA-RICS Executive Director
Joann Huerta, LA-RICS Committees Secretary

AGENDA ITEM A

NOTE: ACTION MAY BE TAKEN ON ANY ITEM IDENTIFIED ON THE AGENDA

I.   CALL TO ORDER

Technical Committee Vice-Chair Tab Rhodes called the meeting to order at 1:37 p.m.

II.   ANNOUNCE QUORUM – Roll Call

Committee secretary Joann Huerta took roll call for each committee and both committees had quorum.

III.   APPROVAL OF MINUTES (A)

A.   May 22, 2018 – Regular Meeting Minutes

Operations Committee Vice-Chair Tab Rhodes asked for a motion to approve the minutes. Committee Member Cathy Chidester moved to approve first, seconded by Technical Committee Chair Ted Pao.

Ayes 9:   Zuniga, Pao, Iwanaga, Chidester, Rhodes, Buard, Walczak, Leyn and England

IV.   PUBLIC COMMENTS – (NONE)

V.   CONSENT CALENDAR – (NONE)

VI.   REPORTS (B-C)

B.   Status Report Update for LTE

Steve Sidore, Broadband Consultant with Televate, provided an update on the Long Term Evolution (LTE) Public Safety Broadband Network (PSBN).

There has been progress on the transition of the LTE network. As of July 1, 2018, AT&T has taken over the site equipment. LA-RICS is working with AT&T to connect those sites to the FirstNet / AT&T core network while ensuring minimal to no disruption for the public safety users. A "toy cell" for testing was configured at one of the maintenance locations. APN (Access Point Name) testing for connections to the agencies was successfully concluded last week.

Last night AT&T cut over the first site, and they are currently in the process of completing the testing of various APNs including the APN for Los Angeles County Fire (Fire) and Sheriff Departments and other Member Agencies that worked with

AGENDA ITEM A

AT&T. In the next phase, AT&T will transfer the rest of the sites. They are currently going through an internal AT&T investigation on how to do this.

There is service contact work that is being done by ISD relating to pricing agreements at the local level / public safety contract. There is a current contract for public safety communications with FirstNet/AT&T through National Association of State Procurement Officers (NASPO) which was executed by Nevada to establish FirstNet pricing which local users could consider utilizing for pricing. Another aspect of the LA-RICS transition work is Agency device migration and we are currently working with AT&T on that process.

Technical Vice-Chair Scott England asked the cost and is it an official contract we can utilize? Mr. Sidore stated that the NASPO is an official contract, but needs to be adopted by the local agency intending to utilize it, such as the County of Los Angeles.   Technical Vice-Chair England stated that LACoFD has a NASPO contract that was approved by county, but the Nevada NASPO would have to be approved.

Executive Director Scott Edson, stated that before September 1, 2018, we should have Los Angeles County pricing for AT&T and FirstNet services available to you anything outside of the agency would be able to peer off that same vehicle. They are evaluating bids and they are expected to include AT&T FirstNet services among others for primary and extended primary users.

C.   Status Report Update for LMR

Program Manager Delfino provided a Powerpoint presentation that included a map/visual to illustrate sites that are in construction and those active and planned and provided details supporting the construction-related activities occurring at these sites to date.

Active LMR Site Work June 2018 – UASI 16 Work are listed below:

1. CCB: Ph.4, Ph.2 change work
2. FCCF: Ph.4
3. HPK: Ph.4, Ph.2 change work
4. LA-RICS-HQ: Ph.2
5. LDWP243: Ph.4
6. MMC: Ph.4
7. ONK: Ph.4, Ph.2 change work
8. PLM: Ph.4   - Milestone – CORE Connection to FCCF
9. POM: Ph.1 Geo-tech generator
10. SPN: Ph.1 Geo-tech tower scheduled 6/28/18

AGENDA ITEM A

11. TPK: Ph.4
12. VPK: Ph.2

The next sites on the PowerPoint presentation are listed below:

- LA-RICSHQ - (rack delivery for this site)
- LDWP243 – (RF fingerprint, completed tower, stacked generator and this is a finished site)

Project Manager Delfino acknowledge Motorola on their quality of finished work to these sites.

- MMC – (drone technology was utilized to take this view of the tower, antennas and shelter installed)
- TPK – (180 foot tower structure, shelter and generator all installed. Glendale Water and Power Vault Location scheduled to install and complete Ph. 2 Under UASI 16))

The next sites on the PowerPoint presentation are the 20/20/20/20 Track:

Sites with targeted start dates for the end of summer 2018

1. UCLA
2. POM
3. LA-RICSHQ
4. SGH
5. LAN
6. UNIV
7. CRN
8. DPW038

Sites with targeted start dates for the end of Year 2018

1. BHS
2. RHT
3. MIR
4. OAT
5. AGH
6. LACFDEL
7. INDWT

This concluded the Program Manager's Report and there was no further discussion.

AGENDA ITEM A

VII. DISCUSSION ITEMS – (D)

D. Traveling Meeting Mobile

Operations Committee Vice-Chair Lieutenant Tab Rhodes stated that LA-RICS would like our Committee Members to host some of our future meetings at member agency locations so we can bring LA-RICS to them and showcase deployments and technologies. Operations Chair Kyle Zuniga stated having the meeting close to a site and visit twice a year will show Members what LA-RICS is doing.

VIII. ADMINISTRATIVE MATTERS – (E-G)

E. APPROVE RECOMMENDATION TO THE LA-RICS JOINT POWERS AUTHORITY BOARD OF DIRECTORS TO APPROVE THE LA-RICS SECURITY POLICIES (POLICY NOS. 025-2018 AND 026-2018)

Deputy Program Manager Tanya Roth presented Agenda Item E, explaining that the policies before Committees were in follow up to the overall Information Technology Security Program Policy that was presented and approved at the May 22, 2018, meeting. The Security Program Policy (024-2018) set forth the definitions, roles and responsibility for the LA-RICS security program with the intent that that there would be forth coming policy on specific topics. Policy 025-2018 covers responsible and ethical use of LA-RICS information technology resources and policy 026-2018 sets forth antivirus protocol.

Member Mike Iwanaga inquired as to who would be the Chief Information Security Officer. Deputy Program Manager Roth responded stating that Technical Chair Ted Pao is earmarked for the role, but she also clarified that it's not currently applicable since LMR sites are not yet active. Technical Vice-Chair England stated that it would be nice if the role was a one-year term that rotated to different agencies.

Member Iwanaga stated that it's a two year out and will be up and running. Member Cathy Chidester stated the other thing to think about is Cyber security insurance which is a contract that they use. Deputy Program Manager Roth stated that as LA-RICS wrote these policies they wanted them to be firm enough to protect LA-RICS. LA-RICS has the ability to amend them as needed with the appropriate approval. At this time, we recommended that the Joint Operations and Technical Committee:

Approve a recommendation to the Board to adopt the following LA-RICS security policies to enhance the Authority's Information Technology (IT) Security Program:

- Board Policy No. 025-2018 – Use of LA-RICS Information Technology Resources Policy (Enclosure 1)

AGENDA ITEM A

- Board Policy No. 026-2018 – LA-RICS Antivirus Security Policy (Enclosure 2)

Member Leyn motioned first, seconded by Member Chidester.

Ayes 9:   Zuniga, Pao, Iwanaga, Chidester, Rhodes, Buard, Walczak, Leyn and England

MOTION APPROVED

IX.   **MISCELLANEOUS – (NONE)**

X.   **ITEMS FOR FUTURE DISCUSSION AND/OR ACTION BY THE COMMITTEE**

XI.   **CLOSED SESSION REPORT – (NONE)**

XII.   **ADJOURNMENT AND NEXT MEETING:**

Operations Committee Vice-Chair Rhodes announced adjournment of this meeting at 2:02 p.m., and the next Committee Meeting is on Tuesday, September 25, 2018, at 1:30 p.m., location forthcoming.

LOS ANGELES REGIONAL INTEROPERABLE COMMUNICATIONS SYSTEM AUTHORITY

LA-RICS

2525 Corporate Place, Suite 100
Monterey Park, California 91754
Telephone: (323) 881-8291
http://www.la-rics.org

SCOTT EDSON
EXECUTIVE DIRECTOR

September 25, 2018

Joint Operations and Technical Committee Members
Los Angeles Regional Interoperable Communications System Authority (the "Authority")

Dear Committee Members:

APPROVE RECOMMENDATION TO THE LA-RICS JOINT POWERS AUTHORITY BOARD OF DIRECTORS TO APPROVE THE LA-RICS' SECURITY POLICIES (POLICY NOS. 027-2018 AND 028-2018)

SUBJECT

Request from the Joint Operations and Technical Committees to recommend certain LA-RICS security Policies, attached hereto, be presented to the Joint Powers Authority (JPA) Board of Directors (Board) with a recommendation to approve and adopt the policies.

RECOMMENDED ACTIONS

It is recommended the Joint Operations and Technical Committees:

Approve a recommendation to the Board to adopt the following LA-RICS security policies to enhance the Authority's Information Technology (IT) Security Program:

- Board Policy No. 027-2018 – LA-RICS Information Technology Physical Security Policy (Enclosure 1)

- Board Policy No. 028-2018 – LA-RICS Information Technology Risk Assessment and Audit Compliance Policy (Enclosure 2)

AGENDA ITEM E

BACKGROUND

On May 22, 2018, your Committees approved a recommendation to adopt Policy No. 024-2018 (LA-RICS Information Technology and Security Program Policy) that established a security program to ensure that the Authority's IT resources are protected against all forms of unauthorized access, use, disclosure, or modification. Policy No. 024-2018 was the first policy, in a series of policies, presented to your Committees as part of the Authority's IT Security Program. If the recommended actions are approved, the enclosed policies will be presented to the Board for consideration and will add to the Authority's IT Security Program.

PURPOSE/JUSTIFICATION OF RECOMMENDED ACTION

Approval of the recommended action will move the items to the Board for consideration and adoption for inclusion into the Authority's IT Security Program for the protection and use of Authority IT Resources.

It is necessary to implement Policy No. 027-2018 (LA-RICS Information Technology Physical Security Policy) to ensure Authority IT Resources are protected by security measures that prevent physical tampering, damage, theft, or access.

With respect to Policy No. 028-2018 (LA-RICS Information Technology Risk Assessment and Audit Compliance Policy), this policy is necessary in order to ensure the performance of periodic Information Technology (IT) risk assessments of Authority IT Resources in order to identify security threats and security vulnerabilities. Further, this policy would also initiate appropriate audits for compliance with all LA-RICS IT Security policies, standards, and procedures.

Authority staff is working to develop subsequent security policies that will become part of the Authority's IT Security Program to present to this Joint Operations and Technical Committees for consideration. The expectation is to secure Joint Operations and Technical Committees' approval for these policies as well as other security policies that may be interrelated and present cohesive policies packages to the Board for approval. As a result, in the coming meetings, your Committees may see more of these IT security policies presented for consideration.

FISCAL IMPACT/FINANCING

The activity contemplated in the recommended action has no fiscal impact at this time.

FACTS AND PROVISIONS/LEGAL REQUIREMENT

Counsel to the Authority has reviewed the recommended action.

AGENDA ITEM E

CONCLUSION

Upon the Committees' approval of the recommended action, Authority staff will present the policies to the Board coupled with additional interrelated security policies previously approved by your Committees for Board adoption and implementation.

Respectfully submitted,

SCOTT EDSON
EXECUTIVE DIRECTOR

JA
M:\LA-RICS POLICIES\Policy No. 027-2018 (LA-RICS Information Technology Physical Security Policy)\Joint Tech and Ops (09-25-18)\1 Tech Ops Letter_LARICS IT Physical Security and Risk Assess and Audit Policies.docx

Enclosures

c: Counsel to the Authority

AGENDA ITEM E

LA-RICS POLICIES

POLICY TITLE		POLICY NO.
LA-RICS Information Technology Physical Security Policy		027-2018
APPROVED BY	EFFECTIVE DATE	DATE LAST REVISED
LA-RICS JPA Board of Directors	---	---

1.0 PURPOSE

To establish an LA-RICS Information Technology (IT) Security policy to ensure that IT Resources are protected by security measures that prevent physical tampering, damage, theft, or access.

2.0 DEFINITION

As used in this Policy No. 027-2018, the following terms shall have the same meaning as set forth in LA-RICS Policy No. 024-2018 Information Technology and Security Program.

- Authority IT Resources, hereinafter referred to as "IT Resources"
- Authority IT Security Incident, hereinafter referred to as "IT Security Incident"
- Authority IT User, hereinafter referred to as "User"
- Chief Information Security Officer, hereinafter referred to as "CISO"

3.0 POLICY

Proper Identification
Access to areas with IT Resources containing confidential information or personal information shall be physically restricted. Each person in these areas shall wear an identification badge on their outer garments, so that both the picture and information on the badge are clearly visible.

Access to Restricted IT Areas
Restricted IT areas include, without limitation, data centers, computer rooms, telephone closets, network router and hub rooms, voicemail system rooms, and similar areas containing IT Resources. All access to these areas shall require authorization by LA-RICS management and shall be appropriately restricted.

AGENDA ITEM E - ENCLOSURE 1

Physical Security Controls

A User is considered a custodian for any particularly assigned IT Resource(s). If an item is damaged, lost, stolen, borrowed, or otherwise unavailable for normal business activities, the User shall promptly inform the CISO or his/her designee.

IT Resources containing confidential information or personal information located in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access.

If feasible, IT Resources owned by LA-RICS shall be marked with some form of identification that clearly indicates it is the property of LA-RICS.

Each User is responsible for notifying the CISO as soon as an IT Security Incident is suspected.

4.0 COMPLIANCE

Authority personnel who violate this Policy No. 027-2018 may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-Authority personnel who violate this Policy No. 027-2018 may be subject to termination of contractual agreements, denial of access to Authority IT Resources, and other actions as appropriate (i.e. cure letter), as well as both civil and criminal penalties.

5.0 POLICY EXCEPTIONS

Requests for exceptions to this Policy No. 027-2018 shall be reviewed by the CISO and shall require approval by the Executive Director. Users requesting exceptions shall provide such requests to the CISO.

The request should specifically state the following:

a.   Scope and justification for the exception
b.   Potential impact or associated risk upon granting the exception
c.   Risk mitigation measures to be undertaken by the Authority
d.   Initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein

The CISO shall review such requests, confer with the requestor, and refer the matter to the Executive Director for action.

AGENDA ITEM E - ENCLOSURE 1

POLICY TITLE	POLICY NO.
LA-RICS Information Technology Physical Security Policy	**027-2018**

References:

- ▪ LA-RICS Policy No. 021-2017 (Cybersecurity Incident Response)
- ▪ LA-RICS Policy No. 024-2018 (Information Technology and Security Program)
- ▪ LA-RICS Policy No. 025-2018 (Use of Information Technology Resources, including the Acceptable Use Agreement)

AGENDA ITEM E - ENCLOSURE 1

POLICY TITLE		POLICY NO.
LA-RICS Information Technology Risk Assessment and Audit Compliance Policy		**028-2018**
APPROVED BY	EFFECTIVE DATE	DATE LAST REVISED
LA-RICS JPA Board of Directors	---	---

1.0 PURPOSE

To ensure the performance of periodic Information Technology (IT) risk assessments of IT Resources in order to identify security threats and security vulnerabilities and also to initiate appropriate audits for compliance with all LA-RICS IT Security policies, standards, and procedures.

2.0 DEFINITION

As used in this Policy No. 028-2018, the following terms shall have the same meaning as set forth in LA-RICS Policy No. 024-2018 Information Technology and Security Program.

- Authority IT Resources, hereinafter referred to as "IT Resources"
- Authority IT Security, hereinafter referred to as "IT Security"
- Authority IT User, hereinafter referred to as "User"
- Chief Information Security Officer, hereinafter referred to as "CISO"

3.0 POLICY

The CISO and/or his/her designee shall periodically conduct and document an IT risk assessment and audit process. IT risk assessments encompass information gathering, analysis, and determination of security vulnerabilities within IT Resources and IT business practices.

IT risk assessments are necessary to analyze and mitigate security threats to IT Resources, which may come from any source, including, but not limited to, natural disasters, disgruntled employees, hackers, the Internet, and equipment or service malfunction/breakdown.

AGENDA ITEM E - ENCLOSURE 2

IT risk assessments shall be conducted on all IT Resources and any process or procedure by which IT Resources are utilized and maintained. IT risk assessments shall be performed on each facility that house IT Resources.

An IT risk assessment program (e.g., vulnerability scans of networks, systems and applications that identifies risks) shall include an inventory of IT Resources; review of IT Resource policies, standards, and procedures; review of IT Security policies, standards, and procedures; assessments and prioritization of security threats to, and vulnerabilities within IT Resources; and implementation of safeguards to mitigate any identified threats and/or vulnerabilities within IT Resources.

The CISO shall conduct or coordinate an audit of Users' compliance with IT Resources policies, standards and procedures, and IT Security policies, standards, and procedures. Audits shall be prioritized and scheduled based on risk determined by the CISO.

4.0   COMPLIANCE

Authority personnel who violate any LA-RICS policies related to IT Resources and/or IT Security may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-Authority personnel who violate these same policies may be subject to termination of contractual agreements, denial of access to IT Resources, and other actions as appropriate (i.e. cure letter), as well as both civil and criminal penalties.

5.0   POLICY EXCEPTIONS

Requests for exceptions to this Policy No. 028-2018 shall be reviewed by the CISO and shall require approval by the Executive Director. Users requesting exceptions shall provide such requests to the CISO.

The request should specifically state the following:

a.   Scope and justification for the exception
b.   Potential impact or associated risk upon granting the exception
c.   Risk mitigation measures to be undertaken by the Authority
d.   Initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein

The CISO shall review such requests, confer with the requestor, and refer the matter to the Executive Director for action.

AGENDA ITEM E - ENCLOSURE 2

References:

- LA-RICS Policy No. 021-2017 (Cybersecurity Incident Response)
- LA-RICS Policy No. 024-2018 (Information Technology and Security Program)
- LA-RICS Policy No. 025-2018 (Use of Information Technology Resources, including the Acceptable Use Agreement)