Silicon Valley Regional Interoperability Authority
EComm Users Group

EComm User Agreement & Security Policy

29 October 2010
Revised 8 June 2011

Preface

EComm is a private microwave network connecting all Public Safety Answering Points (9-1-1 centers), selected key public safety facilities and numerous radio sites throughout Santa Clara County. Built largely with grant funding, EComm provides secure data and voice communications to public safety agencies and other cooperating agencies for mission critical applications. EComm is owned and operated by the Silicon Valley Regional Interoperability Authority, a joint powers agreement agency.

This document sets forth policies for use of EComm by Santa Clara County, the fifteen cities and towns, and those special districts and educational institutions which are approved by the SVRIA Board of Directors.

Section I hereof comprises a user agreement defining the process for requesting EComm bandwidth, user responsibilities, appropriate network use, expectations for network performance and problem identification and resolution.

Section II sets forth applicable security policies and requirements for EComm use.

Section I – EComm User Agreement

EComm Network Description

1. Definition of EComm Resources – EComm consists of a monitored hot standby loop in north county and a monitored hot standby backbone in south county with spurs to various locations. A System Block Diagram (SBD) is maintained to depict current system topology. A copy of the current SBD is available to SVRIA members upon request.

EComm resources include all microwave radios, related site infrastructure, and system routers and firewalls. Whether located at remote sites or in agency facilities, all EComm resources are owned by SVRIA and maintained by SVRIA staff or contractors. Power, environmental conditioning, and equipment room and rooftop space are provided by the agency or site owner at its expense.

2. Definition of Eligible Users – Eligible EComm users, referred to as agencies or users hereinafter, include the first responder agencies of SVRIA members and other governmental entities that perform a first responder mission as defined in Homeland Security Presidential Directive 8, Section 2(d).

3. EComm Use Criteria – To be eligible for transport via EComm, applications must meet the following criteria:

A. Support mission critical public safety operations. Examples include CAD-to-CAD, dispatch and incident radio communications, and GIS systems that provide real time operational context to first responders and

B. Are transaction based and designed to efficiently utilize network bandwidth,

C. Or judged to be mission critical in the event of a disaster or an incident which impacts public networks such as the public switched telecommunications network (PSTN) and the Internet. Examples include fiber or copper cable cuts, major earthquake damage and acts of terrorism impacting the public telecommunications infrastructure.

4. Network Operations Center – SVRIA will operate or contract for operation of a Network Operations Center (NOC) which will provide system monitoring including the services listed in Appendix A hereto.

Network Applications

5. EComm Application Request Process – Agencies will complete an EComm Application Request form and submit it as an email attachment to the SVRIA Executive Director and the EComm Users Group Chair. The current form is attached hereto as Appendix B.

Requests received by mid-month will be reviewed at the next monthly Users Group meeting. Agency staff should be prepared to support their request at that meeting. Requests which meet EComm use criteria and are consistent with available transport bandwidth will be recommended to the Executive Director for approval prior to the next Users Group meeting.

Recommendations for approval by the Executive Director may be contingent upon specific conditions including but not limited to application testing, equipment acquisition, permit issuance, external agency approval, network availability, etc.

Requests which are not approved by the Executive Director may be appealed to the SVRIA Working Committee at its next meeting.

6. External Agency Approvals – When the approval of an external agency (e.g., DOJ for CLETS) is required to authorize the sharing or exchange of data via EComm, the requesting agency will request the necessary approval(s) prior to submitting its EComm Application Request. The Users Group may issue a recommendation of approval contingent upon such external approval(s). In either case, a copy of the submitted or issued external agency approval document must be attached to the Application Request.

If the external agency requires periodic renewal of approvals, that condition must be noted in the Application Request and will form the basis of periodic reviews as defined in Section I – Paragraph 7 hereof.

7. Sunset Provision – Each approved EComm application shall specify, on its Application Request form, a date of or event triggering expected termination if one is known by the requester. The EComm Users Group will calendar a review of such applications ninety days prior to the expected termination date. Approved applications without expected termination dates will be calendared for review by the Users Group every two years on the anniversary of the application's start of transport via EComm or sooner if required by external agency approval.

Major upgrades of EComm transported applications or the implementation of a successor system shall be communicated to the Users Group together with an estimate of resulting changes in network utilization. Such notifications shall trigger a review of the application. Renewed recommendations of approval of the Users Group will be required prior to implementation of the upgrade or new system.

Agencies operating approved EComm transported applications will have the opportunity to present to the Users Group their plans for application termination or continuation and to explain the impact of application upgrades or changes.

Periodically, the Users Group shall report to the Working Committee the status of all applications including current and expected application usage, estimated network utilization, known problems, planned changes or upgrades, and impacts on other applications and network availability. If an approved application is a candidate for removal from the EComm network for reasons other than planned termination, the Users Group will make a recommendation to the Executive Director with the rationale for removal. Recommendations for removal approved by the Executive Director may be appealed to the Working Committee at its next meeting.

Network Use

8. Agency Approval of Application Users – Agencies are responsible for the identification, training and management of its application users. The organization(s) and number of users for each requested application will be specified in the Application Request Form (example: fire department; 160 users).

Any change in the number of organizations or changes of more than 50% in the number of individual users for an approved application will be communicated by email in advance to the Users Group Chair. The Users Group will review the proposed change and may make a recommendation to the Executive Director to approve or deny the change.

9. Agency Use Responsibilities – Each agency is responsible for the users of its approved applications. Data transport via EComm is limited to that necessary to run the approved application. Any other use of EComm of prohibited.

10. Data Ownership and Retention – Each agency shall own its data transported via EComm and shall apply its own data retention policy to that data. The NOC shall be responsible for system-wide data such as network configurations which shall be owned by SVRIA. Periodically updated backup copies of system-wide data shall be maintained by Santa Clara County and San Jose.

11. Public Network Connectivity – Agency owned networks that are used to access the EComm network may also have connections to public networks such as the Internet provided that each agency's public network security infrastructure and network connections are physically and logically independent from the EComm provided network infrastructure installed at their location. That is, the user owned firewall or network security device facing the EComm owned firewall shall be physically separate and independent from any user network security device attached to a public network. There will be no exceptions to this policy.

12. Remote Access – Data transported via EComm and transmitted through any public network segment, wireless network, unsecured network or the public Internet shall be immediately protected with encryption over such segment(s) or network(s). The encryption shall meet the requirements specified in the FBI's CJIS Security Policy draft version 5.0 section 5.10.1.2 or, if encryption is required by an External Agency as defined in Section I – Paragraph 6 hereof, the encryption shall meet the requirements specified by that External Agency. Encryption keys used to encrypt data transmitted via EComm shall be managed by the user agency.

13. Determination of User Costs – Costs for custom design, hardware, software or site infrastructure required to implement an approved application shall be borne by the user agency. EComm operations, maintenance and replacement costs are borne by SVRIA members in accordance with the cost sharing formula approved by the Board of Directors. An appropriate user fee may be required of approved non-member users.

Network Operation

14. System Availability and Service Level – EComm has been designed to provide 99.999% availability (up to 316 outage seconds per year excluding planned outages) on each path and will be maintained to ensure reliable performance. However, SVRIA provides no guarantee of service level to user agencies.

15. Demarcation Between EComm and Users – EComm network support extends through the EComm owned and managed firewall interface that faces the user agency's connecting firewall or other agency owned network security device. In the event of a service affecting problem, SVRIA or contractor staff will test and troubleshoot up to the agency facing EComm firewall interface and will correct any discovered issues involving the EComm network. SVRIA or contractor staff will make best efforts to assist user agencies in their problem diagnosis and resolution. However, all other testing and problem resolution will be the responsibility of the user agency.

16. Points of Contact – Both SVRIA and each user agency will designate 7x24 technical contacts in sufficient depth to ensure coverage. Appendix C hereto contains the current list of contacts and their telephone numbers.

In the event of a service affecting failure determined to be within the user agency's network, inability to promptly reach that agency's technical contact may result in disconnection from EComm.

SVRIA, the NOC and each agency will maintain a current email distribution, also contained in Exhibit C, to facilitate routine communications including notification of planned outages.

17. Notification of Problems or Outages – The NOC and each user agency has an ongoing responsibility to promptly notify each other of outages or other service affecting problems. Each will provide the other with 14 calendar days notice of planned outages including changes in user environments which may generate fault or other alerts and messages at the NOC. The NOC will provide each user agency with timely updates on the resolution of unplanned outages or other problems. Agencies will advise the NOC when user environments are restored.

18. Issue Resolution Process – The following process will be used to elevate any EComm related issue which is not resolved to the user's satisfaction. Step 1 is to bring the unresolved issue to the EComm Users Group by requesting that the issue be added to the next meeting agenda by the Users Group Chair. In the event that the issue is not resolved at the next Users Group meeting, Step 2 is to address the issue to the SVRIA Executive Director who will respond prior to the following Users Group meeting.

19. Access to EComm Equipment – Each agency will provide access to EComm equipment for SVRIA or contractor staff including after-hour access. Agencies may impose reasonable security practices but may not prohibit access.

20. Emergency Operations Mode – In the event of a disaster or other emergency resulting in the activation of the Santa Clara Operational Area EOC, EComm bandwidth may be restricted to some or all users. Such disruption in service will be limited to non-voice communications and only for the minimum duration consistent with the nature of the event.

Section II – EComm Security Policies & Requirements

Hardware

1. Demarcation Between EComm and Users – The demarcation between the EComm network and user agencies is the EComm owned and managed firewall interface that faces the user agency's connecting firewall or other agency owned network security device. EComm network operation will be monitored and managed by the EComm NOC up to that connection.

2. EComm Firewall Operation – The EComm owned and managed firewall will be configured to provide minimum access between the EComm firewall and the connected network which is adequate to support the application(s) being accessed. Management of the EComm firewall will be provided by the EComm NOC and changes to the EComm firewall will be approved by the EComm Users Group.

3. User Firewall Operation – The user owned firewall or network security device shall be physically separate and independent from any user network security device attached to a public network. The user firewall shall be configured to provide minimum access between the user network and the EComm network which is adequate to support the application(s) being accessed. Management of the user firewall is the responsibility of the user agency. *[Revised 8 June 2011 to delete language requiring User Group approval of user agency firewall changes.]*

Software

4. Standards for Protocols and Technologies – EComm is a TCP/IP system currently running IP Version 4 but is capable of being upgraded to Version 6.

5. Encryption – If a user application requires encryption, it is the responsibility of the connecting agencies to provide, at their cost, encryption capability and to provide any certificates and associated equipment.

Change Control

6. Process Description – Prior to running any new application over the EComm network or implementing any modification to an existing EComm transported application, user agencies shall follow the process described in Section I – Paragraph 5 hereof.

Connectivity

7. Internet Generated Traffic – Agency owned networks that are used to access the EComm network may also have connections to public networks such as the Internet provided that each agency's public network security infrastructure and network

connections are physically and logically independent from the EComm provided network infrastructure installed at their location. There will be no exceptions to this policy.

8. Wireless Device Generated Traffic – Data transported via EComm and transmitted through any public network segment, wireless network, unsecured network or the public Internet shall be immediately protected with encryption over such segment(s) or network(s). The encryption shall meet the requirements specified in the FBI's CJIS Security Policy draft version 5.0 section 5.10.1.2 or, if encryption is required by an External Agency as defined in Section I – Paragraph 6 hereof, the encryption shall meet the requirements specified by that External Agency. Encryption keys used to encrypt data transmitted via EComm shall be managed by the user agency.

Security

9. User Device Security – User agencies shall implement and maintain physical access control to limit use of EComm transported applications to agency employees and authorized agents. Further, user agencies shall implement and maintain logical access control of one tier or greater authentication, unique to each user, such as secure passwords or smart cards or their equivalent.

10. Virus and Malware Protection – All user systems with EComm connectivity shall maintain anti-virus updates (including scanning engines and signature files) current to within seventy-two hours (three calendar days) of their availability. In the event of a recognized and publicized security risk, user agencies shall make their best effort to immediately obtain and install all appropriate patches and anti-virus updates to EComm transported applications.

11. Immediate Notification of Incidents – User agencies shall immediately notify the EComm NOC of any security violation – security incident, virus infection, or attempted or successful intrusion – defined in this document or which, in the judgment of the user, may in any way impact EComm network security.

Appendix A
Network Operations Center (NOC) Services

To be updated

1. IP Performance and Capacity Management
   - Capacity monitoring, review and analysis
   - Trend identification for proactive problem resolution
   - Use history based recommendations to reduce maintenance and performance issues
   - Performance reporting (e.g., bandwidth utilization, network availability, etc.)

2. MPLS Service Provisioning
   - Facility and network availability verification
   - Circuit or route verification and conflict identification
   - Manage data-fill requirements and circuit or route alarms
   - Completion reporting

3. Change Management
   - Manage change and configuration process
   - Enforce accepted change management process
   - Maintain system block diagram

4. Sustaining Engineering
   - Synchronization of NOC with network changes
   - Update NOC procedures to accommodate SVRIA staff requests

5. Call Management
   - Single point of contact for SVRIA and field engineers
   - Dispatching of on call field technicians
   - Track and record dispatch progress and actions
   - Track and record hardware change-outs

Note: It is anticipated that the NOC services provider will offer time & material priced support to user agencies for firewall configuration or other related services.

Appendix B
EComm Network Application Request Form

APPLICATION / SYSTEM information				
Application/System Name:				
Requesting Agency/Dept:			Executive Sponsor/Reviewer:	
Document Date/Version	Date:	Version:	Exec Sponsor/Reviewer's Phone No.	
Author's Name			Author's Phone Number:	
Author's Email Address:				
Project Priority (provide only if multiple application requests are submitted):			__ of __	

Please check all that apply:

a. E-Comm Approval Request

- □ New Application/System
- □ Update/Modify Existing Application/System
- □ Connect to/Expand E-Comm Network

b. Point of Connection

- □ Existing E-Comm Access Point
- □ Adds New Microwave Link/Spur (licensed/unlicensed)
- □ Adds new leased T1 link
- □ Adds new leased fiber link

c. Application/Service Type

- □ Voice
- □ Data
- □ Voice and Data
- □ Public Safety
- □ General Government
- □ Special District / Other

1. <u>Application/System Description:</u>

- Briefly describe the application and its purpose in operational terms.
- Describe typical users (law, fire, medical, emergency management, etc.).
- Explain how the application fits EComm transport requirements:
  - o Transaction based and designed to efficiently utilize network bandwidth.
  - o Supports mission critical public safety operations, and/or
  - o Will be mission critical in the event of a disaster incident impacting public networks.
- Explain connectivity requirements (DS0, DS1, Ethernet, encryption or other security needs), data packet size, transport frequency, number of end users/agencies across system, transport frequency (continuous/intermittent/random/scheduled), maintenance response requirements, and loading impact on system capacity, etc.
- If any external agency approvals required for this application, attach proof of approval.
- Does the application have an anticipated termination date?

2. How will approval of this request enhance and improve operational efficiency, service delivery and/or system reliability for your agency or jurisdiction?

3. If an existing application, explain how connectivity is currently being achieved and why E-Comm transport is being requested (include any potential cost savings that could be achieved and if the savings will be one-time or ongoing).

4. Describe any one-time and ongoing costs associated with adding connectivity to E-Comm and/or moving this application/system onto the E-Comm network for voice/data transport (e.g., one-time programming or other services, labor, equipment, interface, data conversion, maintenance, leased circuit, etc.) and how these activities and associated cost will be addressed.

5. Provide a diagram of how network expansion/connectivity to E-Comm and/or how the application/system voice/data will flow on the E-Comm network (mark-up of existing E-Comm diagram).

6. Desired Outcomes (use bulleted list):
   - (Examples, remove it not applicable) Increases application reliability and/or operational efficiency
   - Enhances and/or expands service delivery for (name agencies or jurisdictions)
   - Generates cost savings
   - Reduction in maintenance

7. Estimated start and completion dates:
   - Desired start date: _____ (Date work begins)
   - Desired completion date: _____ (Date fully operational on E-Comm)

8. Attachments:
   - Diagram application/system voice/data flow on E-Comm network (Item 5). Identify whether physical or logical topology is provided.
   - Equipment inventory list (if applicable)
   - Signed E-Comm User Security Agreement
   - List of authorized agencies requiring access for this application and estimate of total number of users.
   - List of EComm translated IP addresses that correlate to requester's device IP addresses.
   - List of IP addresses of devices on requester's network accessed by other agencies.
   - List of TCP or UDP ports which need to be allowed on EComm firewalls.
   - If devices will be accessed by hostname, include the Fully Qualified Domain Name (FQDN) and method of name resolution (local DNS or DNS zone transfer).
   - Proof of external agency approval, if required.

Appendix C
Points of Contact

EComm Contact List

Jurisdiction / Agency	7x24 Phone	Data Primary	Data Alternate
Campbell	408 866-2101	Jeff Gershaneck 408-866-2753	Joe McElwain 408-866-2755
Cupertino	--	--	--
Gilroy	408-846-0350	Steve Baty 408-846-0353	Dwane Camp 408-846-0413
Los Altos	650-947-2770	Mike Trautman 650-947-2601	Elizabeth Vargas 650-947-2822
Los Altos Hills	--	--	--
Los Gatos	408-354-8600	John Zore 408-761-4524	Chris Gjerde 408-760-5430
Milpitas	408-586-2420	Bill Marion 408-586-2701	Matthias Schwarz 408-586-2711
Morgan Hill	408-779-2101	Jeff Rosenberger 408-779-7271 x229	Mike Fumagalli 408-779-7271 x459
Monte Sereno	--	--	--
Mountain View	650-903-6395	Doug Kiner 650-903-6833	Jeff Goss 650-903-6859
Palo Alto	650-329-2413	Glenn Loo 650-329-2492	Lisa Bolger 650-329-2654
Saratoga	--	--	--
Santa Clara	408-261-5455	Help Desk 408-261-5455	Tom Torres 510-205-0315
San Jose	#1 408-799-8437 #2 408-655-3668	Vijay Sammeta 408-535-3565	Ed Kim 408-655-3668
Sunnyvale	408-730-7185	Jose Rodenzo 408-730-7552	Will Guitarte 408-730-2729
Santa Clara County	408-918-7000	Dean Linebarger 408-918-7055	Pat Doolan 408-918-4711
Sheriff's Office	408-808-4739	Bruce Overoye 408-808-4660	Yosh Mikosz 408-808-4661
Water District	408-690-0982	Chris Cannard 408-265-2600	Will Hutchinson 408-265-2600