BayLoop User Agreement & Security Policy
11 April 2014

Preface

BayLoop is a private microwave network connecting all Public Safety Answering Points (9-1-1 centers), Emergency Operations Centers (EOCs) selected key public safety facilities and numerous radio sites throughout the San Francisco Bay Area. Built largely with grant funding, BayLoop provides secure data and voice communications to public safety agencies and other cooperating agencies for mission critical applications. BayLoop is owned and operated by the seven Counties (Alameda, Contra Costa, Marin, San Francisco, San Mateo, Santa Clara and Solano) that have agreed to host BayLoop facilities (the BayLoop Counties). Maintenance and network monitoring support is currently provided by the Bay Area Regional Interoperable Communications Systems Joint Powers Authority (BayRICS).

This document sets forth policies for regional use of BayLoop by the BayLoop Counties, BayRICS member agencies, and other counties, municipalities, special districts and educational institutions that are approved by the BayRICS Board of Directors.

Section I of this document comprises a user agreement defining the process for requesting BayLoop 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 BayLoop use.

Section I – BayLoop User Agreement

BayLoop Network Description

1. Definition of BayLoop Resources – BayLoop consists of a monitored hot standby loop which rings the San Francisco Bay Area. A System Block Diagram (SBD) is maintained to depict current system topology. A copy of the current SBD is available to BayRICS members upon request.

BayLoop resources include all microwave radios, related site infrastructure, and system routers and firewalls located at remote sites or in agency facilities. All BayLoop resources are owned by the BayLoop Counties, with regional maintenance and monitoring provided by BayRICS. 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 BayLoop users, referred to as agencies or users hereinafter, include the first responder agencies of the BayLoop Counties, BayRICS

members and other authorized governmental entities that perform a first responder mission as defined in Homeland Security Presidential Directive 8, Section 2(d).

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

A. Support mission critical public safety operations. Examples include, but are not limited to, CAD-to-CAD, dispatch and incident radio communications, and GIS systems that provide real time operational context to first responders; or

B. Are 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, but are not limited to, fiber or copper cable cuts, major earthquake damage and acts of terrorism impacting the public telecommunications infrastructure; and

C. Are transaction based and designed to efficiently utilize network bandwidth.

4. Network Operations Center – BayRICS 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.

5. BayLoop Work Group. Each BayLoop County shall designate one primary representative and one alternate to serve on the BayLoop Work Group. The Work Group is primarily responsible for making recommendations to the BayRICS General Manager regarding BayLoop network applications requests and other regional operations, policy and security matters. Each Work Group member shall have one vote on Working Group actions. Alternates may vote only when the primary member is not present.

The BayRICS General Manager shall serve as the Chair of the Working Group and shall facilitate all Work Group meetings, prepare meeting agendas, schedule network applications requests and present all Work Group recommendations to the BayRICS Technical Advisory Committee (TAC) and/or BayRICS Board in a timely fashion. The BayRICS General Manager is a non-voting member of the Work Group; however, the General Manager shall have the authority to cast a tie-breaking vote in cases of Work Group deadlock.

The Work Group shall schedule regularly monthly meetings at a time and place approved by the Work Group. The Work Group Chair may schedule additional meetings at other times as necessary. If no action is required, the Chair may cancel the regular monthly meeting.

Network Applications

6. BayLoop Application Request Process – Agencies will complete a BayLoop Application Request form and submit it as an email attachment to the BayRICS General Manager and the BayRICS TAC Chair. The current form is attached hereto as Appendix B.

Requests received by mid-month will be reviewed at the next monthly BayLoop Work Group meeting. Requesting Agency staff should be prepared to support their request at that meeting. Requests which meet BayLoop use criteria and are consistent with available transport bandwidth will be recommended to the General Manager for approval at the next TAC meeting.

Recommendations for approval by the General Manager 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 General Manager or protests of approved requests may be appealed to the BayRICS Board of Directors at its next meeting.

7. 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 BayLoop, the requesting agency will request the necessary approval(s) prior to submitting its BayLoop Application Request. The TAC 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.

8. Sunset Provision – Each approved BayLoop application shall specify, on its Application Request form, a date of or event triggering expected termination if one is known by the requester. The Work 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 Work Group every two years on the anniversary of the application's start of transport via BayLoop or sooner if required by external agency approval. The TAC may waive or modify this requirement in its initial approval action if the circumstances dictate.

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

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

Periodically, the BayRICS General Manager and TAC shall report to the Board of Directors on 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 BayLoop network for reasons other than planned termination, the TAC may make a recommendation to the General Manager with the

rationale for removal. Recommendations for removal approved by the General Manager may be appealed to the Board of Directors at its next meeting.

Network Use

9. 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 BayRICS General Manager and TAC Chair. The Work Group will review the proposed change and may make a recommendation to the General Manager to approve or deny the change.

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

11. Data Ownership and Retention – Each agency shall own its data transported via BayLoop 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 BayRICS. Periodically updated backup copies of system-wide data shall be maintained by BayRICS.

12. Public Network Connectivity – Agency owned networks that are used to access the BayLoop 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 BayLoop provided network infrastructure installed at their location. That is, the user owned firewall or network security device facing the BayLoop 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.

13. Remote Access – Data transported via BayLoop 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 BayLoop shall be managed by the user agency.

14. 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. BayLoop operations, maintenance and monitoring costs are borne by BayRICS

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

15. System Availability and Service Level – BayLoop 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, BayRICS provides no guarantee of service level to user agencies.

16. Demarcation Between BayLoop and Users – BayLoop network support extends through the BayLoop 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, BayRICS or contractor staff will test and troubleshoot up to the agency facing BayLoop firewall interface and will recommend actions to correct any discovered issues involving the BayLoop network. BayRICS 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.

17. Points of Contact – Both BayRICS 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 BayLoop.

BayRICS, 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.

18. 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.

19. Issue Resolution Process – The following process will be used to elevate any BayLoop related issue which is not resolved to the user's satisfaction. Step 1 is to bring the unresolved issue to the TAC by requesting that the issue be added to the next meeting agenda by the TAC Chair. In the event that the issue is not resolved at the next TAC meeting, Step 2 is to address the issue to the BayRICS General Manager who will respond prior to the following TAC meeting.

20. Access to BayLoop Equipment – Each agency will provide access to BayLoop equipment for BayRICS 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, BayLoop 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 – BayLoop Security Policies & Requirements

Hardware

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

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

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 BayLoop network which is adequate to support the application(s) being accessed. Management of the user firewall is the responsibility of the user agency.

Software

4. Standards for Protocols and Technologies – BayLoop 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 BayLoop network or implementing any modification to an existing BayLoop 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 BayLoop 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 BayLoop provided network infrastructure installed at their location. There will be no exceptions to this policy.

8. Wireless Device Generated Traffic – Data transported via BayLoop 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 BayLoop 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 BayLoop 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 BayLoop 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 BayLoop transported applications.

11. Immediate Notification of Incidents – User agencies shall immediately notify the BayLoop 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 BayLoop 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 BayRICS staff requests

5. Call Management
   - Single point of contact for BayRICS 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
BayLoop 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. BayLoop Approval Request

- ☐ New Application/System
- ☐ Update/Modify Existing Application/System
- ☐ Connect to/Expand BayLoop Network

b. Point of Connection

- ☐ Existing BayLoop 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. Application/System Description:

   - Briefly describe the application and its purpose in operational terms.
   - Describe typical users (law, fire, medical, emergency management, etc.).
   - Explain how the application fits BayLoop transport requirements:
     - Transaction based and designed to efficiently utilize network bandwidth.
     - Supports mission critical public safety operations, and/or
     - 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 BayLoop 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 BayLoop and/or moving this application/system onto the BayLoop 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 BayLoop and/or how the application/system voice/data will flow on the BayLoop network (mark-up of existing BayLoop 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 BayLoop)

8. Attachments:
   - Diagram application/system voice/data flow on BayLoop network (Item 5). Identify whether physical or logical topology is provided.
   - Equipment inventory list (if applicable)
   - Signed BayLoop User Security Agreement
   - List of authorized agencies requiring access for this application and estimate of total number of users.
   - List of BayLoop 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 BayLoop 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

BayLoop Contact List

Jurisdiction / Agency	7x24 Phone	Data Primary	Data Alternate