Secure Video Conferencing for the Federal Government: What Every Agency Needs to Know

In recent years the quality, performance and cost of video conferencing has dramatically improved, making it a viable communications tool across the federal government. From distance learning to telework and inter- and intra-agency collaboration, high-definition (HD) video conferencing systems are being used within a majority of federal civilian agencies and departments, all branches of the U.S. military and throughout the Department of Defense (DoD).

Video conferencing has proven to be a cost-saving and effective means to ensure staff is "trained and ready" and a viable alternative to in-person meetings. In fact, in June 2011, the U.S. House of Representatives announced plans to use video conferencing as a means to conduct face-to-face meetings with constituents and to foster better engagement with the public while reducing costs related to traveling. Video conferencing also goes hand-in-hand with important government programs and has become a critical technology to support telework mandates, green initiatives and continuity of operations (COOP) plans.

During this evolution, government entities and standards bodies have identified strict government security requirements to protect these critical communication and collaboration tools from being compromised. While it is much more challenging to compromise the security of a videoconference call than a transaction, it is clear that video conferencing must be a secure endeavor.

Video conferencing systems must be architected with HD quality calls in mind, and support the highest levels of security typically demanded by government agencies and the military. In these types of environments, the security is not commercially available and the open Internet is not a viable option. Support for government-grade secure technologies and infrastructure, demonstrated compliance with strict government security and interoperability standards, and built-in management and administrative features are essential.

This white paper examines key components of secure video conferencing systems for the federal government, including:

- **Encryption**
- **Firewalls**
- **ISDN networks**
- **Secured switching and video conferencing over satellite**
- **Built-in security features**
- **Compliance with government security and interoperability standards**

Encryption

Encryption is the process of transforming information to make it unreadable to anyone except those possessing the cryptographic key. Long used by the DoD to facilitate secret communication, encryption is now a commonly used technology within many federal civilian agencies to protect information. Encrypting data in transit is an added layer of protection since it can be difficult to physically secure access to all networks or electronic communications.

LifeSize®, a key innovator and leader in HD-based video conferencing, strongly recommends using Advanced Encryption Standard (AES) for video conferencing calls. While some vendors' systems and legacy architectures can experience degradation in video quality or performance while processing resources are performing the encryption algorithm, this is not the case with LifeSize. Fundamentally, LifeSize believes that customers should not have to choose between security and the highest quality, most immersive communication experience for users. Because of the performance advantages of the purpose-built, LifeSize HD architecture, users can take advantage of the industry's highest quality video and audio while operating with encryption. Performing encryption does not require any tradeoffs in functionality or limit performance.

The purpose-built full HD architecture of LifeSize® Room 200™ and LifeSize® Room 220™ supports AES enabled point-to-point calls and multiparty calls with up to four sites in continuous presence in full HD 720p60 and 1080p30 quality. This is true whether customers choose to use the H.323 protocol or the SIP protocol for their video communications. In addition, all LifeSize encryption is standards-based and can interoperate with other platforms.

Firewalls

Firewalls have become an essential part of securing federal agency networks and are widely used to block unauthorized access while permitting authorized communications. All data entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. Firewalls can be implemented in either hardware or software, or a combination of both, and can be configured to permit, deny, encrypt, decrypt or proxy all computer traffic between different security domains based upon a set of rules and other criteria.

Video conferencing calls must be able to interoperate with firewalls to maintain security policies (such as preventing unauthorized video conferencing users from accessing private networks, i.e. intranets) while providing secure video conferencing calls inside and outside of the agency. This enables secure

communications with mobile users and teleworkers, as well as with other agencies, departments and third-parties, such as contractors, around the globe. The challenge is that conducting H.323/SIP video conferencing calls requires the opening and closing of communication ports, potentially leaving networks vulnerable to attacks and security issues.

Examples of firewall and NAT implementations. Some firewalls have multiple attributes:
i. Packet Filtering: This method looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly common, effective and transparent to users.
ii. Application Gateway: This method applies security mechanisms to specific applications, such as Telnet and FTP servers. This is very effective, but can degrade performance in some implementations.
iii. Circuit-level Gateway: This method applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
iv. Proxy Server: This method intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.
v. NAT: Network address translation (NAT) is a general term for techniques that establish and maintain TCP/IP network connections traversing NAT gateways. NAT is often used in conjunction with firewalls. NAT enables the use of a range of IP addresses internally, while sharing a smaller range of public IP addresses. Internal users will be able to see the public video conferencing, but the public video conferencing users can't see individual devices on the internal side of the NAT.
vi. DMZ: A DMZ or demilitarized zone is another segment of a LAN and is a subnetwork that contains and exposes an organization's external services to a larger, untrusted network. A DMZ adds an additional layer of security to a LAN so that an external hacker only has access to equipment in the DMZ, rather than the whole of the network. Video conferencing endpoints can be deployed in the LAN on the WAN (not recommended because they can be attacked) or in a DMZ.

One typical way to address firewall and network address translation (NAT) gateways is with an enterprise-class firewall and NAT traversal solution that supports tunneling. This approach enables the user to maintain high quality video and audio communication and ensure strong security while traversing a firewall in keeping with the agency's security policies.

As an example, LifeSize offers a product called LifeSize® Transit™. It enables end points to communicate with each other through firewalls without the need for intermediate nodes or unsafe opening of communications ports.

When looking for a firewall or NAT traversal option, it is important to select a standards-based solution that is easy to use and manage. In the case of LifeSize Transit, it supports both H.323/H.460 and SIP/STUN-TURN-ICE.

Video endpoints should be preconfigured and ready for use with the firewall and NAT traversal solution. All

LifeSize endpoints are enabled with standards based H.460 and STUN-TURN-ICE software, out of the box at no additional cost.

Where the firewall is deployed is another key consideration. Often an agency's IT organization will deploy firewalls in the demilitarized zone (DMZ). The DMZ should be setup to only allow traffic in/out on ports 1720 (H.323 signaling), 5060 (SIP signaling) and user configurable ports. This will ensure the SSH, SNMP and HTTP/HTTPS ports are not open to attack. If the IT organization prefers a LAN deployment and chooses to not use Static NAT, then LifeSizeTransit can be used for firewall/NAT traversal.

ISDN Networks

Integrated Services Digital Network (ISDN) has traditionally been a secure environment for the simultaneous digital transmission of voice, video, data and other network services over traditional circuits of the public switched network. Multiple B-channels and in some cases multiple switches make it very difficult to intercept an ISDN video call.

While most networks are moving to an IP H.323 network, legacy equipment within the DoD and federal government agencies require the use of ISDN, creating a mixed IP and ISDN environment. Interoperability is extremely important to ensure that new HD video conferencing equipment can support legacy systems. The LifeSize Networker is able to communicate to legacy equipment via Primary Rate (PRI) or Basic Rate (BRI) circuits to support ISDN and mixed environments.

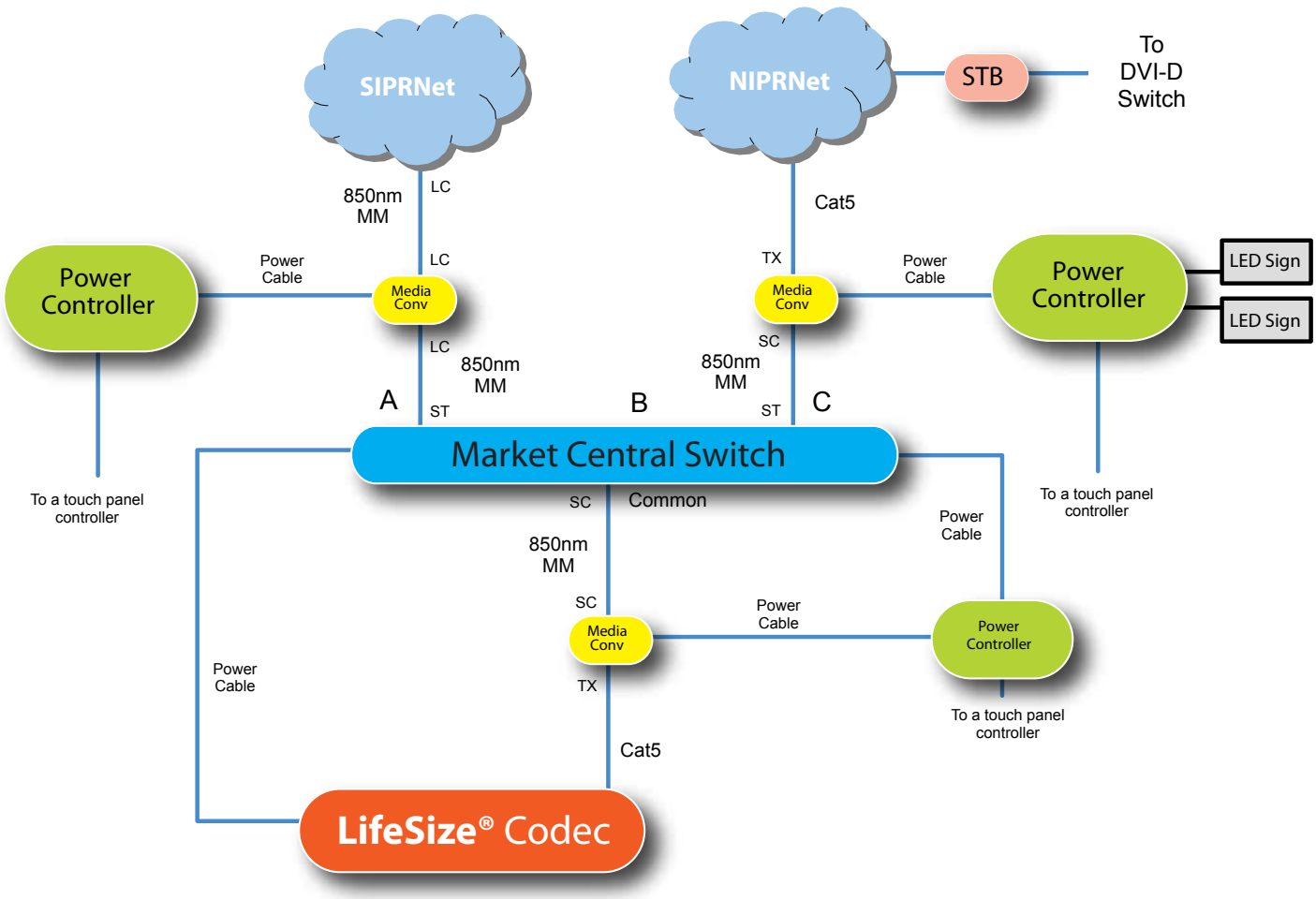
Secured Switching and Video Conference over Satellite

Secured Switching in the DoD environment involves the use a single codec for Secret Internet Protocol Router Network (SIPRnet) and Non-secure Internet Protocol Router Network (NIPRnet), classified and unclassified. A LifeSize codec connects to both secured and non-secured environments. The network (SIPRnet or NIPRnet) connects to a third-party DISA-approved media convertor, which in turn connects to a third-party DISA-approved A/B switch (such as a Market Central Switch). The A/B switch connects to a third party DISA-approved media convertor, which connects to a LifeSize codec. During this switching one opposite media convertor is turned off ensuring security. For example, when SIPRnet is in use the media convertor connected to the NIPRnet is powered off ensuring the NIPRnet cannot communicate with the SIPRnet. Typically these systems are controlled by a third-party touch panel so that the switching is seamless to video conference system users.

Another secure communications network in the DoD is the Joint Worldwide Intelligence Communications System (JWICS), a 24-hour a day network designed to meet the requirements for secure (TS/SCI) multimedia (voice, video and graphics) intelligence communications worldwide. LifeSize video conferencing systems operate in a JWICS environment through media convertors that connect to the LifeSize codec.

Effective and secure communication and collaboration with deployed soldiers, sailors, airmen and marines is essential to national security. High quality video conferencing over secure, third-party satellite networks to mobile devices provides critical support to the warfighter. Through the Joint User Interoperability Communications Exercise (JUICE) LifeSize has proven that its codecs work in a low bandwidth environment

and provide better resolution and a better video conferencing experience than other devices. Specific tests were conducted to demonstrate point-to-point video conferencing calls via satellite to a mobile van and multipoint video calls via satellite to a mobile van and boat. LifeSize is able to communicate via H.323 and SIP and connect under multiple video standards: H.261, H.263, H.263+, H.264 and H.239. Users are able to see a noticeable improvement in the quality of communications when compared to other video conferencing systems.



Built-in Security Features

In order to meet DoD security requirements, HD video conferencing systems must be designed from inception to include standards-based security capabilities. This means that in addition to supporting secure technologies and infrastructure and interoperability standards, systems must also include built-in management and administrative features to enable secure procedures. LifeSize video conferencing solutions offer extensive capabilities to set and enforce secure best practices and policies. These include:

Account Management
Use of tiered user accounts
Configurable banners & backgrounds

Password Management
Ability to change all default passwords
Numeric passwords
Disallowing repetitive use of same password
Password protection via SHA-1 hash

Session Management
Ability to enable/disable FIPS 104-2
Ability to enable/disable HTTP
Ability to enable/disable SSH
Ability to enable/disable Telnet
Ability to enable/disable SNMP
Ability to enable/disable H.235 AES Security

Encryption
Use of FIPS-140 validated encryption on all management and media streams
Real-time encryption of media via 128-bit or 256-bit AES
Storage of sensitive data using SHA-1 hash (one-way encryption)

Certificates
Manual support for installation of DoD-backed certificates for the integrated HTTPS server

Backup and Recovery
Support for offloading of audit logs
Ability to backup and restore of system configurations on FTP servers (for fast recovery from outages)
Ability to revert to hardware-level factory settings

Compliance with Government Security and Interoperability Standards

Video communications solutions for use in government and military applications require special certifications and security credentials. Commitment by the vendor to an active product evaluation and certification program to demonstrate compliance with strict government security standards is a critical component when evaluating video conferencing systems.

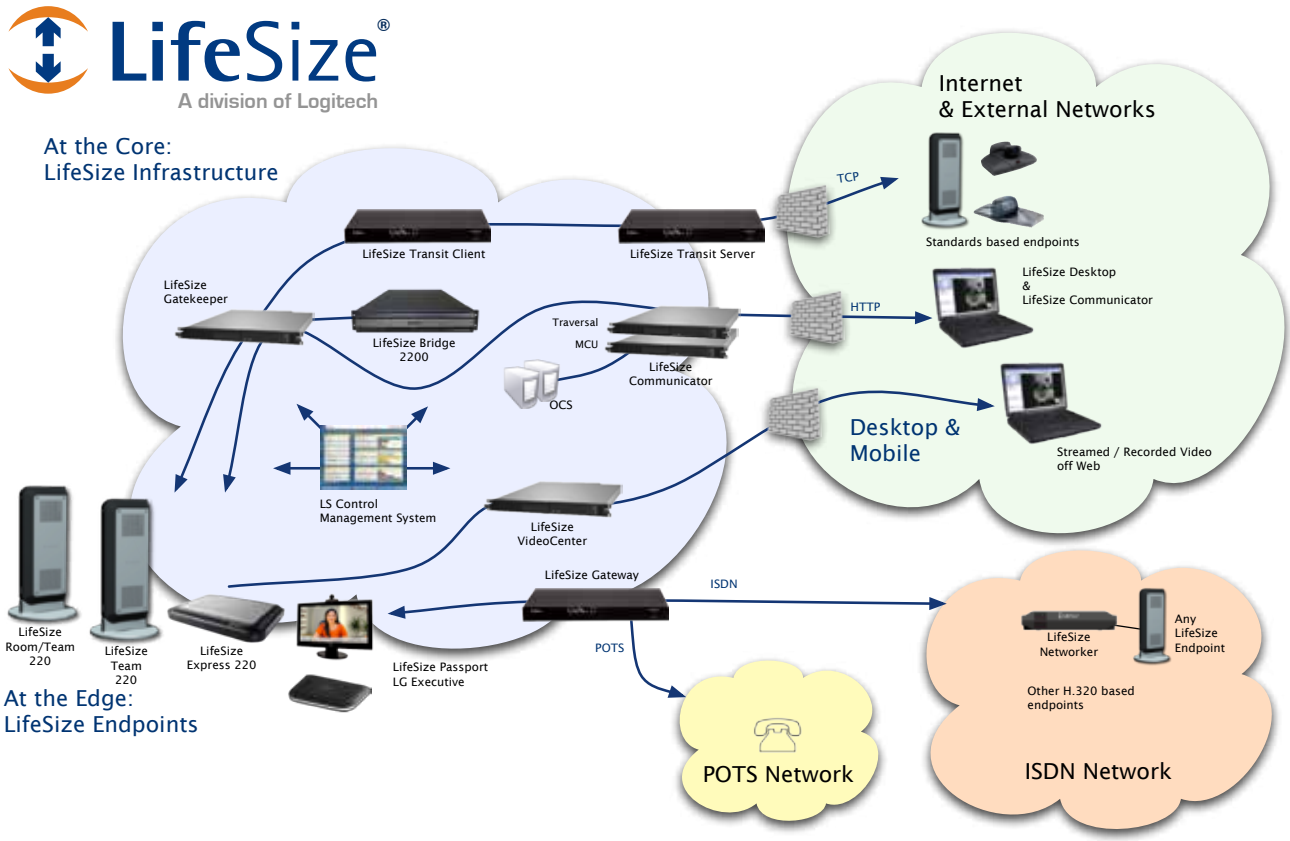
Depending on the requirements, the following standards or credentials apply:

a. Security
- Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States Federal Government for use by all non-military government agencies and by government contractors. Many FIPS standards are modified versions of standards used in the wider community (ANSI, IEEE, ISO, etc.).
- H.235 AES designates support for 128-bit encryption without degradation in HD video and audio quality or performance.
- H.460 and SIP overcome the challenges NATs and firewalls create for multimedia communication within and across agencies and third-parties.
- Approved Products Lists (APL) are maintained by branches of the U.S. Military and DoD. Products on these lists have successfully passed comprehensive and rigorous security testing programs and have been approved for use by a particular service branch and may be fielded in DoD networks.
- The U.S. Army Certificate of Networthiness (CoN) accreditation ensures products meet strict U.S. Army and DoD standards for security, compatibility and sustainability.

b. Interoperability
- Joint Interoperability Test Command (JITC) provides a full-range of interoperability testing evaluations and certification services to support rapid acquisition and fielding of global net-centric war-fighting capabilities.IPv6 testing completion indicates a product satisfies the U.S. federal government IPv6 test requirements (USGv6) to ensure interoperability among all IT and networking components used to build, maintain and secure the IT infrastructure of federal agencies.
- Approved Products List (APL) are also created for products that successfully pass comprehensive and rigorous interoperability testing programs.
- Joint User Interoperability Communications Exercise (JUICE) is an annual worldwide U.S. DoD exercise sponsored by the Executive Agent Theater Joint Tactical Networks and hosted by the U.S. Army CECOM Life Cycle Management Command Software Engineering Center to evaluate new or emerging technologies in a Joint Task Force (JTF) operational environment.
- Certified Support for Microsoft Unified Communications Platforms indicates that the solution can interoperate with this popular UC platform used widely across the federal government to seamlessly connect a variety of communications services – including email, video, chat and phone – from a single user interface.

Security	Interoperability
• FIPS 140-2 for both FIPS CAVP and FIPS CMVP • H.235 AES • Support for H.460 and SIP solutions • Inclusion on the Army Approved Products List (APL) • CoN for the Army (in process)	• Joint Interoperability Test Command (JITC) certifications including Interoperability Certification (IOC) and Information Assurance (IA) accreditation • IPv6 testing program completion • Inclusion on the DoD Unified Capabilities Approved Products List (UC APL) • JUICE 11 demonstrating DoD and DHS interoperability in support of a JTF • Support for Microsoft® UC Platforms • DevConnect Tested status demonstrating support for Avaya Aura® UC systems

VTC over a Secured Network



Conclusion

The cost and complexity of video conferencing systems have dropped dramatically in recent years, while performance and quality have increased. As government agencies and departments explore the applications and benefits of HD video conferencing, security is a key requirement for any deployment. LifeSize video conference solutions address government's rigorous standards with support for encryption and firewalls, interoperability with legacy and modern networks, and control with administrative and management tools to enforce security policies. As government agencies conduct research on the security aspect of today's HD video conferencing systems, key questions to ask include:

- Will performing encryption require any tradeoffs in functionality or limit performance?
- How does the video conferencing system interoperate with firewalls and NAT gateways to maintain security policies?
- Does the video conferencing system operate seamlessly within ISDN and mixed IP and ISDN environments?
- Has the solution demonstrated it can handle secured switching within the DoD environment?
- What level of voice and video quality and performance can be expected over secure third-party satellite communications networks?
- Does the system include built-in management and administrative capabilities to set and enforce security policies? How easy are they to use?
- What standards and credentials for security and interoperability does the video conferencing system support?

LifeSize works closely with federal agencies and defense organizations to help them deliver on their missions with HD video conferencing solutions that offer the quality, price, security, interoperability and performance they demand.

To learn more, book a demo at:
www.lifesize.com/Request_A_Demo.

GSA Schedule Contract: GS-35F-0582V
TAX ID: 061680606
DUNS#: 131001369
Cage Code: 55HQ4

LifeSize® A division of Logitech

AMERICAS:
LifeSize
1601 S. MoPac Expressway
Suite 100
Austin, Texas 78746 USA

+1 512 347 9300
Toll Free US +1 877 543 3749
E-mail info@lifesize.com
www.lifesize.com

EMEA:
LifeSize Regional Office
+49 89 1222 899 0 (Germany)
Toll Free Europe 00 8000 999 09 799

APAC:
LifeSize Regional Office
+65 6303 8370 (Singapore)