



March 28, 2016

VIA ELECTRONIC FILING

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Notice of Ex Parte – *Use of Spectrum Bands Above 24 GHz for Mobile Radio Services* – GN Docket No. 14-177

Dear Ms. Dortch:

On March 24, 2016, Joseph Sandri and Christopher Naoum of FiberTower Spectrum Holdings, LLC (“FiberTower”), along with Douglas Brandon and Steven Rowings of Akin Gump Strauss Hauer & Feld LLP, met with the following staff of the Federal Communications Commission (“Commission”) in the above-captioned proceeding: John Schauble, Brian Regan, Tim Hilfiger, Simon Banyai, Catherine Schroeder, Nancy Zaczek, and Matthew Pearl of the Wireless Telecommunications Bureau; Serey Thai of the Office of Engineering and Technology; Jose Albuquerque of the International Bureau; and Ahmed Lahjouji of the Public Safety and Homeland Security Bureau.¹

In the meeting, FiberTower discussed the importance of ensuring the resiliency and security of 5G networks deployed over the millimeter wave (“mmW”) band spectrum, as described more fully in the attached materials. In particular, FiberTower emphasized the need for mission-critical networks to be physically diverse and independently powerable to ensure ongoing operations in the event of natural or man-made disruptions to a portion of the network. FiberTower also discussed the measures that can be taken to ensure that 5G communications are physically secure, such as by exclusive licensing to prohibit use of certain frequencies by any party other than the licensee and by unique device configurations that preclude access to the communications by devices outside the network. FiberTower and the staff then discussed the importance of encrypting the communications themselves to further ensure their security. Additionally, FiberTower discussed its support for the concept of “security by design,”

¹ Tim Hilfiger and Serey Thai participated in the meeting via phone.



Security & Millimeter Wave Exclusively Licensed Wide-Area Spectrum: 5G Access and Backhaul

Potent security configurations and strategies exist for carrier-class, 'wireless fiber' broadband fixed, portable and mobile connectivity over exclusively licensed, wide-area spectrum authorizations in the 24GHz and 39GHz bands. These robust, multi-layered techniques provide excellent security milestones for any organization seeking to rely on these bands for 5G data transmissions.

I. GENERALLY

Physical layer barriers utilizing this particular configuration of carrier-grade or government-grade wireless fiber (fixed wireless) *generally* include, and are not limited to:

- Exclusively-licensed spectrum bands. Access to a license holder's spectrum is illegal without specific, FCC-approved, contractual and regulatory authorizations.
- There are marketplace and regulatory barriers to successfully obtain and operate proprietary equipment capable of operation in exclusively licensed bands. The manufacturers know who owns the exclusive licenses.
- Even if equipment can be procured that operates over exclusively-licensed wide-area spectrum, there are very specific bands, and also multiple specific channels and sub-channels within various spectrum bands, upon which a particular piece of equipment can operate.
 - Equipment is specific to a channel or set of channels and to a specific manufacturer and model. Without obtaining these specific physical equipment combinations, a specific wireless fiber link cannot operate.
 - Each transceiver (radio) can be physically configured to require specific authentication before it will communicate with any other radio of the same manufacture and model.



- For Point-to-point and multiple-point-to-point narrow beamwidth prevents interference and interception.
 - Exceedingly tight beamwidths in the millimeter band spectrum result in a thin bore-sight ‘pencil beam’ between, for example, two rooftops being served.
 - Those rooftops are typically secured by multiple layers of building management security. Because both ends are controlled by the network operator there are not lengths of fiber or copper underground or in conduit between the two facilities potentially available to be tapped.
 - If wireless fiber interception is attempted (for example via crane or helicopter), typically the physical link drops due to obstruction. Also physically placing a bore-sight system into the beam in order to attempt interception typically automatically triggers various alarms concerning main-lobe or side-lobe interference.
- For point-to-multipoint sector and omni-directional base stations servicing fixed, portable or mobile devices, the signal will ‘bathe’ entire areas. The above-listed physical barriers to accessing the signal are able to be supplemented by extensive encryption and spread-spectrum style channel movement.
- HTTPS, SSH, SNMP v3, and RADIUS support for controlled device access
 - HTTPS is the protocol for secure communications over a computer network that is widely used over the internet. It encrypts the user communications with web interfaces such as Chrome, Explorer, etc.
 - Secure Shell (SSH) provides a secure channel over an unsecured network.
 - Simple Network Management Protocol (SNMP) and other configurations provide added protection layers.¹
 - Each packet over a secure HTML interface is encrypted and packed with a message authentication code (MAC) and is bolstered by Secure Socket Layer (SSL), Transport Layer Security (TLS), Authentication, RSA key exchange.

II. CONFIGURATION

¹ Password history protocols to avoid re-use; configurable password expiration; configurable SNMP access (disable, read-only [RO], read-write [RW]), etc.



Each transceiver (radio) is hard-configured to communicate only with a matched radio of the same make and model. At installation, each link is programmed with the MAC and IP address of its partner, and specific link numbering, channel assignment, polarization², power-flux-density, QAM and other factors are individually tailored to the individual link. Then the two ends of the link will communicate only with each other, eliminating “man-in-the-middle” attacks. The pre-pairing also allows fast deployment as all that is needed is power for the modules to start searching for each other. Over-the-air security is achieved through a proprietary scrambling mechanism that cannot be disabled or spoofed by commercial tools. On transmission, the typical proprietary system signal often passes through the following representative processes:

- Reed Solomon forward error correction where added bits are applied
- Scrambling with a code that repeats every eight Reed Solomon code words
- Interleaver where the signal is then changed in order
- Convolutional Encoding where the signal is scrambled into two streams and then sent serially with some bits unsend
- The signal is coded onto one of BPSK, QPSK, 16 QAM, 64 QAM, 128 QAM, 256 QAM, 512 QAM, 1024 QAM, 2048 QAM or 4096 QAM waveforms
- Then the signal is interleaved across a specific waveform model (such as 1024-carrier OFDM)

FIPS 197 compliant, 128- or 256-bit AES Encryption (or other optional software encryption models) are available and routinely applied.³ Additional encryption of data before it is transmitted is possible (and often routinely added) by using the security measures built into routers, network devices and web sites in order to ensure end-to-end protection of data. Finally, it is critical to reinforce that as a service provider offering a secure private line

² Beam forming and polarization dynamics can be configured to defeat unwanted signal connectivity. Beyond traditional vertical and horizontal polarizations, there are now radial polarization techniques that, when combined with timing codes, can act a strong deterrents.

³ FIPS 197 compliant AES encryption options provide (1) low latency (add about 4 micro seconds), (2) full-rate encrypted Gigabit or Fast Ethernet performance under all traffic loads, (3) cipher block chaining (128—bit blocks) conceal patterns in plain text.



broadband link, if and when any data leaves the confines of the secured system and is, for example, sent to another system (via the Internet, etc), it is inherently no longer secure.

Sources: FiberTower laboratory, Motorola, SAF, DragonWave, Bridgewave, and National Spectrum Managers Association (NSMA).

FiberTower Labs

5G mmWave Security: First Principles



Physically-Diverse Network Infrastructure

Follow the Existing Federal Standard

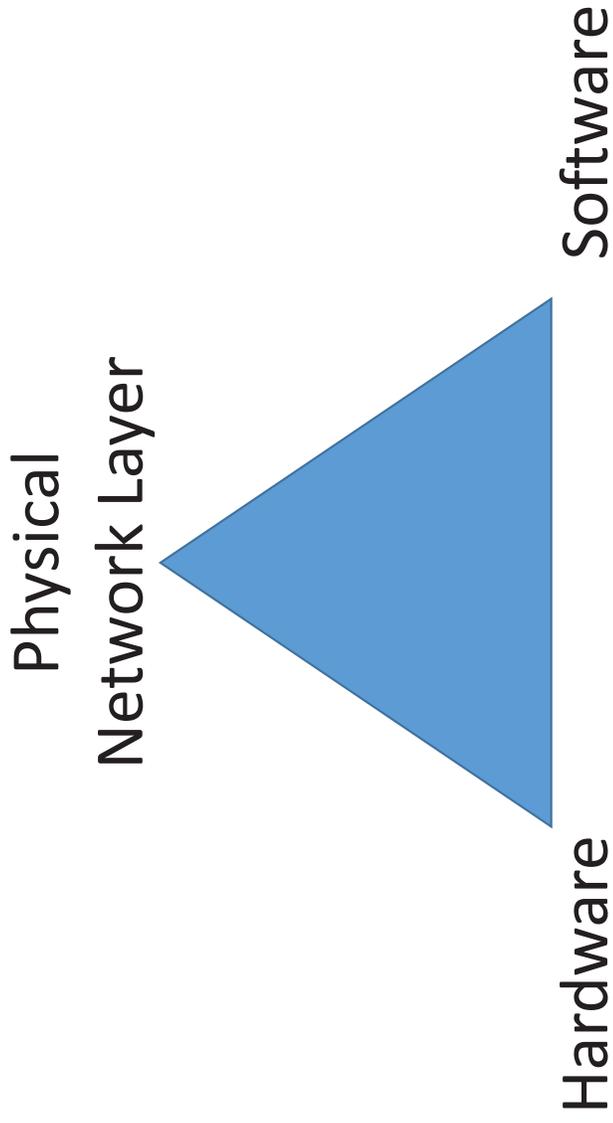
- Physical Diversity Standard – Pub Law 108-447, Section 414 (See also GSA Network Contract).
 - Service Locations: Physically Diverse Ingress and Egress
 - *Network A* should enter and exist the service location at least 20' from physically-diverse *Network B*
 - Rights-of-Way: *Network A* Must Use Rights of Way Between Service Locations That Are Physically-Diverse From *Network B*.
 - Separation of at least 20'.
 - Switching Centers: *Network A* Must Use A Switching Center That Is Physically-Diverse From *Network B*.

Independently Powerable:

Network A and *Network B* should not be reliant on the same power grid. If they are, the critical network elements should be independently powerable (generator; battery; alternatives)



Deploy TRIAD Barriers: Best-in-Class Standards for Each Barrier Element



TRIAD: Sample Barrier Elements

- **Cyber Security Protection TRIAD**
 - **Physical Network Layer Barriers**
 - Physically-Diverse Networks, Pub. Law 108-447, Section 414.
 - OMB Memo M-15-13
 - Exclusively licensed bands
 - Marketplace and regulatory barriers to obtaining equipment to operate in the exclusively-licensed bands
 - Encryption by Layering: Licensed and Unlicensed bands are very broad and there are (i) multiple channels, (ii) multiple elevation angles, and (iii) multiple polarizations on which broadband 5G links can operate. Thus mobile, multipoint and point-to-point broadband network signals can essentially coded to be layered over a multiplicity of physical delivery options
 - Horizontal, Vertical, and Radial Polarization Options
 - For point-to-point connectivity to mission-critical sites, physically intercepting a pencil thin beam is much more challenging than accessing and intercepting wireline.



TRIAD: Sample Barrier Elements Summary (CONT'D)

- **Cyber Security Protection TRIAD**
 - **Hardware Security Barriers**
 - Radio brands and models are almost always not interchangeable by physical design. Moreover, models of the same radio brand cannot communicate with either end of a link without first being specifically configured to do.
 - Configurations require such differentiators as channel, subchannel, polarization, modulation, polarization, and other variables.
 - Without such configurations, effective interception is often defeated.
 - **Encryption Via Software Security Barriers**
 - HTTPS, SSH, SNMP v3, and RADIUS support for controlled device access
 - Encryption: FIPS 197 and 140 Compliance and other encryption protocols easily overlaid



THANK YOU!





EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 8, 2015

M-15-13

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Tony Scott
Federal Chief Information Officer

SUBJECT: **Policy to Require Secure Connections across Federal Websites and Web Services**

This Memorandum requires that all publicly accessible Federal websites and web services¹ only provide service through a secure connection. The strongest privacy and integrity protection currently available for public web connections is Hypertext Transfer Protocol Secure (HTTPS).

This Memorandum expands upon the material in prior Office of Management and Budget (OMB) guidance found in M-05-04² and relates to material in M-08-23³. It provides guidance to agencies for making the transition to HTTPS and a deadline by which agencies must be in compliance.

Background

The unencrypted HTTP protocol does not protect data from interception or alteration, which can subject users to eavesdropping, tracking, and the modification of received data. The majority of Federal websites use HTTP as the as primary protocol to communicate over the public internet. Unencrypted HTTP connections create a privacy vulnerability and expose potentially sensitive information about users of unencrypted Federal websites and services. Data sent over HTTP is susceptible to interception, manipulation, and impersonation. This data can include browser identity, website content, search terms, and other user-submitted information.

¹ Publicly-accessible websites and services are defined here as online resources and services available over HTTP or HTTPS over the public internet that are maintained in whole or in part by the Federal Government and operated by an agency, contractor, or other organization on behalf of the agency. They present government information or provide services to the public or a specific user group and support the performance of an agency's mission. This definition includes all web interactions, whether a visitor is logged-in or anonymous.

² <https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-04.pdf> "Policies for Federal Agency Public Websites"

³ <https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf> "Securing the Federal Government's Domain Name System Infrastructure."

To address these concerns, many commercial organizations have adopted HTTPS or implemented HTTPS-only policies to protect visitors to their websites and services. Users of Federal websites and services deserve the same protection. Private and secure connections are becoming the Internet's baseline, as expressed by the policies of the Internet's standards bodies⁴, popular web browsers, and the Internet community of practice. The Federal government must adapt to this changing landscape, and benefits by beginning the conversion now. Proactive investment at the Federal level will support faster internet-wide adoption and promote better privacy standards for the entire browsing public.

All browsing activity should be considered private and sensitive.

An HTTPS-Only standard will eliminate inconsistent, subjective determinations across agencies regarding which content or browsing activity is sensitive in nature, and create a stronger privacy standard government-wide.

Federal websites that do not convert to HTTPS will not keep pace with privacy and security practices used by commercial organizations, and with current and upcoming Internet standards. This leaves Americans vulnerable to known threats, and may reduce their confidence in their government. Although some Federal websites currently use HTTPS, there has not been a consistent policy in this area. An HTTPS-only mandate will provide the public with a consistent, private browsing experience and position the Federal Government as a leader in Internet security.

What HTTPS Does

HTTPS verifies the identity of a website or web service for a connecting client, and encrypts nearly all information sent between the website or service and the user. Protected information includes cookies, user agent details, URL paths, form submissions, and query string parameters. HTTPS is designed to prevent this information from being read or changed while in transit.

HTTPS is a combination of HTTP and Transport Layer Security (TLS). TLS is a network protocol that establishes an encrypted connection to an authenticated peer over an untrusted network.

Browsers and other HTTPS clients are configured to trust a set of certificate authorities⁵ that can issue cryptographically signed certificates on behalf of web service owners. These certificates communicate to the client that the web service host demonstrated ownership of the domain to the certificate authority at the time of certificate issuance. This prevents unknown or untrusted websites from masquerading as a Federal website or service.

⁴ <https://w3ctag.github.io/web-https/> "The World Wide Web Consortium (W3C)"
<https://www.internetsociety.org/news/internet-society-commends-internet-architecture-board-recommendation-encryption-default> "Internet Society"

⁵ In the context of HTTPS on the web, a certificate authority is a third party organization or company trusted by browsers and operating systems to issue digital certificates on behalf of domain owners.

What HTTPS Doesn't Do

HTTPS has several important limitations. IP addresses and destination domain names are not encrypted during communication. Even encrypted traffic can reveal some information indirectly, such as time spent on site, or the size of requested resources or submitted information.

HTTPS-only guarantees the integrity of the connection between two systems, not the systems themselves. It is not designed to protect a web server from being hacked or compromised, or to prevent the web service from exposing user information during its normal operation. Similarly, if a user's system is compromised by an attacker, that system can be altered so that its future HTTPS connections are under the attacker's control. The guarantees of HTTPS may also be weakened or eliminated by compromised or malicious certificate authorities.

Challenges and Considerations

Site Performance: While encryption adds some computational overhead, modern software and hardware can handle this overhead without substantial deleterious impact on server performance or latency.⁶ Websites with content delivery networks or server software that supports the SPDY or HTTP/2 protocols, which require HTTPS in some major browsers, may find their site performance substantially improved as a result of migrating to HTTPS.

Server Name Indication: The Server Name Indication extension to TLS allows for more efficient use of IP addresses when serving multiple domains. However, these technologies are not supported by some legacy clients.⁷ Web service owners should evaluate the feasibility of using this technology to improve performance and efficiency.

Mixed Content⁸: Websites served over HTTPS need to ensure that all external resources (images, scripts, fonts, iframes, etc.) are also loaded over a secure connection. Modern browsers will refuse to load many insecure resources referenced from within a secure website. When migrating existing websites, this can involve a combination of automated and manual effort to update, replace, or remove references to insecure resources. For some websites, this can be the most time consuming aspect of the migration process.

APIs and Services⁹: Web services that serve primarily non-browser clients, such as web APIs, may require a more gradual and hands-on migration strategy, as not all clients can be expected to be configured for HTTPS connections or to successfully follow redirects.

Planning for Change: Protocols and web standards improve regularly, and security vulnerabilities can emerge that require prompt attention. Federal websites and services should deploy HTTPS in a manner that allows for rapid updates to certificates, cipher choices

⁶ <https://istlsfastyet.com>

⁷ <https://https.cio.gov/sni/> "Server Name Identification"

⁸ <https://https.cio.gov/mixed-content/> "Mixed Content"

⁹ <https://https.cio.gov/apis/> "Migrating APIs"

(including forward secrecy¹⁰) protocol versions, and other configuration elements. Agencies should monitor https.cio.gov and other public resources¹¹ to keep apprised of current best practices.

Strict Transport Security: Websites and services available over HTTPS must enable HTTP Strict Transport Security (HSTS)¹² to instruct compliant browsers to assume HTTPS going forward. This reduces the number of insecure redirects, and protects users against attacks that attempt to downgrade connections to plain HTTP. Once HSTS is in place, domains can be submitted to a “preload list”¹³ used by all major browsers to ensure the HSTS policy is in effect at all times.

Domain Name System Security (DNSSEC): The new policy outlined in this Memorandum does not rescind or conflict with M-08-23, “Securing the Federal Government’s Domain Name System Infrastructure.”¹⁴ Once DNS resolution is complete, DNSSEC does not ensure the privacy or integrity of communication between a client and the destination IP. HTTPS provides this additional security.

Cost Effective Implementation

Implementing an HTTPS-only standard does not come without a cost. A significant number of Federal websites have already deployed HTTPS. The goal of this policy is to increase that adoption.

The administrative and financial burden of universal HTTPS adoption on all Federal websites includes development time, the financial cost of procuring a certificate and the administrative burden of maintenance over time. The development burden will vary substantially based on the size and technical infrastructure of a site. The compliance timeline, outlined in this Memorandum, provides sufficient flexibility for project planning and resource alignment.

OMB affirms that tangible benefits to the American public outweigh the cost to the taxpayer. Even a small number of unofficial or malicious websites claiming to be Federal services, or a small amount of eavesdropping on communication with official U.S. government sites could result in substantial losses to citizens.

Technical assistance provided at <https://https.cio.gov> will aid in the cost-effective implementation of this policy.

¹⁰ <https://https.cio.gov/technical-concepts/#forward-secretcy> “Forward Secrecy”

¹¹ <https://https.cio.gov/resources/> “Resources”

¹² <https://https.cio.gov/hsts>, “Strict Transport Security”

¹³ <https://hstspreload.appspot.com>

¹⁴ <https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf> “Securing the Federal Government’s Domain Name System Infrastructure.”

Guidelines

In order to promote the efficient and effective deployment of HTTPS, the timeframe for compliance, outlined below, is both reasonable and practical. This Memorandum requires that Federal agencies deploy HTTPS on their domains using the following guidelines.

- Newly developed websites and services at all Federal agency domains or subdomains must adhere to this policy upon launch.
- For existing websites and services, agencies should prioritize deployment using a risk-based analysis. Web services that involve an exchange of personally identifiable information (PII), where the content is unambiguously sensitive in nature, or where the content receives a high-level of traffic should receive priority and migrate as soon as possible.
- Agencies must make all existing websites and services accessible through a secure connection¹⁵ (HTTPS-only, with HSTS) by December 31, 2016.
- The use of HTTPS is encouraged on intranets¹⁶, but not explicitly required.

To monitor agency compliance, a public dashboard has been established at <https://pulse.cio.gov>.

Technical Assistance

Please visit <https://HTTPS.cio.gov> for technical assistance and best practices to aid in the implementation of this policy.

For questions regarding this Memorandum, contact Mary A. Lazzeri in the Office of E-Government and Information and Technology at egov@omb.eop.gov with "HTTPS-Only Standard" as the subject line.

¹⁵ Allowing HTTP connections for the sole purpose of redirecting clients to HTTPS connections is acceptable and encouraged. HSTS headers must specify a max-age of at least 1 year.

¹⁶ "Intranet" is defined here as a computer network that is not directly reachable over the public internet.