A Study to Develop the Next Generation Systems Architecture for Radio Spectrum Interference Resolution

Prepared by:

Spectrum and Receiver Performance Working Group*
FCC Technological Advisory Council

Version 1.0
March 9, 2016

* Dale Hatfield (Principal Author), Gregory Lapin (Co-Chair), Lynn Claudy (Co-Chair), J. Pierre de Vries, Geoffrey Mendenhall, David Gurney, Mike Tseytlin.

FCC Liaisons: Matthew Hussey, Julius Knapp, Robert Pavlak

Preface

This preliminary Statement of Work for a Study to Develop the Next Generation Systems Architecture for Radio Spectrum Interference Resolution was prepared by the Spectrum and Receiver Performance Working Group of the FCC's Technological Advisory Council (TAC) and approved at a meeting of the TAC membership on March 9, 2016. This document was prepared to encourage the FCC, other government agencies and the academic and private sectors to facilitate the undertaking of such a study by (a) cooperating in refining and completing the Statement of Work, (b) identifying potential funding sources, (c) establishing a governing structure for overseeing the accomplishment of the work, and (d) identifying potential performers of the tasks identified. The urgent need for the study is described in the Statement of Work included herein. The TAC recommends that the FCC work on its own account, and with other government agencies and the academic and private sectors, to facilitate the undertaking of such a study by engaging in the four activities identified above

Table of Contents

A Study to Develop the Next Generation Systems Architecture For Radio Spectrum Interference Resolution

1. Introduction and Background

The exponential growth in demand for access to and use of the radio spectrum is well documented. It is being driven by (a) a combination of more users using more devices and often consuming more bandwidth per device and (b) the requirements of emerging radio-based systems designed to offer new services important to both government and civilian users. An example of the former is the growth in mobile data. A frequently cited annual report from Cisco Systems[1] stated that global mobile data traffic has grown 4,000-fold over the past 10 years and almost 400-million-fold over the past 15 years. It went on to report that mobile data traffic in 2015 grew by 74 percent globally and by 55 percent in the U.S. The report cites a host of reasons for current and future growth, including the dramatic increase in the amount and technical quality of video traffic conveyed due to the proliferation of advanced multimedia uses. In a recent forecast, Gartner, Inc. projected that the Internet of Things (IoT) would be the fastest growth sector in terms of radio emitters and would reach 21 billion devices by 2020.[2] Other examples of rapidly emerging radio services are new types of aeronautical and space systems including, among many others, unmanned aircraft systems (UAS) and Low Earth Orbiting (LEO) satellites. All of these new systems offer the potential of significant public benefits, but also often present unique challenges in terms of interference issues in both transmitting and/or receiving. Adding to the challenge of trying to accommodate intentional radiators is the growing presence of other electrical and electronic devices that unintentionally or incidentally emit radio waves or that are susceptible to the increased density of radio waves that are present.

From a high-level perspective, spectrum management techniques used in response to this explosion in demand include (a) increased densification in both the frequency dimension (e.g., through reduced guard bands) and the space dimension (e.g., through increased frequency reuse) and (b) following the vision set forth in a 2012 Presidential Council of Advisors on Science and Technology ("PCAST") Report,[3] facilitating dynamic sharing in the time, frequency and space dimensions through the use of sophisticated Spectrum Access Systems that rely upon geo-location data-bases and/or spectrum sensing for their operation.

While these approaches, along with more traditional approaches such as using more sophisticated modulation and signal compression techniques are laudable, they change in fundamental ways the vulnerability of the associated systems to both intentional and

---

[1] Cisco. (2016, Feb. 3). *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020* [Online]. Available: http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf

[2] Gartner. (2015, Nov. 10). *Gartner Says 2.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent from 2015* [Online] Available: http://www.gartner.com/newsroom/id/3165317

[3] President's Council of Advisors on Science and Technology. (2012, Jul.). *Report to the President: Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth* ("PCAST Report") [Online]. *Available at* http://go.usa.gov/k27R

unintentional interference. Although it is hoped that largely voluntary collaboration and coordination between and among Federal agencies and the private sector entities involved will be effective in preventing and resolving most interference incidents in an increasingly dynamic shared spectrum environment, fast and effective interference resolution actions will still be needed in cases involving malicious and non-malicious intentional interference that present an immediate threat to the safety of life and to mission critical systems. Incidents involving unintentional interference (or interference produced by incidental radiation) that pose an immediate threat to the safety of life and mission critical systems or which causes harmful interference to other systems or services may require similar, direct regulatory intervention.

Although the techniques outlined above for keeping up with the explosion in spectrum demand have created radio spectrum interference resolution challenges, many of the same, underlying technological developments that make them possible have also led to dramatically improved capabilities for detecting, classifying/identifying, locating, and reporting sources of interference. In combination, these developments suggest an urgent need for a study that uses modern system engineering tools, analyses, and techniques to develop a vastly improved and better coordinated next generation systems architecture for interference resolution.[4] The need for such an architecture is further propelled by the following:

- Existing and future resources for detecting, classifying/identifying, locating, reporting, mitigating and remediating interference are and will, as a practical matter, continue to be scattered across multiple entities, both public and private.

- Budgetary constraints on public entities (e.g., federal agencies) and cost minimization pressures on commercial entities, suggesting the need to avoid unnecessary duplication of facilities and functions.

- The need to automate interference resolution systems in order to speed responses to serious interference incidents and to reduce costs.

- Recent changes in Federal Communications Commission (FCC) enforcement strategies and priorities as reflected in its recent Order addressing Enforcement Modernization.[5]

Failure to develop the next generation systems architecture could lead to unnecessary and costly over-laps in interference monitoring and location equipment and personnel or, at the other extreme, gaps in equipment and personnel that would slow and reduce the effectiveness of responses to serious interference incidents involving the safety of life and property and homeland defense. Such an architecture would facilitate the ability of today's radio spectrum interference

[4] In the systems engineering design process, systems architecting refers to "the partitioning of a system into components, the defining of interfaces among these components and the processes that govern their changes over time." See Robinson, C. (2013, Apr.). *Big 'A' Systems Architecture* [Online]. Available: http://dau.dodlive.mil/files/2013/04/Robinson.pdf. Systems architecting is also explored in more detail in Section 4.g below.

[5] Federal Communications Commission. (2015, Jul. 16). *In the Matter of Reorganization of the Enforcement Bureau's Field Operations*, FCC 15-81 [Online]. Available: https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-81A1.pdf

resolution systems to evolve efficiently and effectively in the face of rapid technological changes.

Finally, the lack of a next generation systems architecture and any associated inability to (a) limit the number of incidents of harmful and disruptive interference and (b) resolve them quickly when they do occur, could also undermine the value of dynamically shared spectrum to commercial entities and the willingness of Federal government agencies to share their spectrum. This would put into serious jeopardy the presidential goal of making an additional 500 MHz of spectrum available for commercial use by 2020[6] and result in the loss of the substantial economic and social benefits associated with further advances in wireless systems and services.

2. Objective

The objective of this study is to develop the next generation systems architecture for radio system interference resolution in spectrum management that is responsive to the challenges and opportunities outlined above and described in more detail in Section 4 below.

3. Scope of Work

The terms “spectrum management,” “interference resolution,” and “enforcement” are broad in scope and sometimes ambiguous. For the purpose of this study, spectrum management is defined to include both the organizations (such as regulators, multi-stakeholder groups, trade associations and operators) and activities (from rulemaking to monitoring and remediation) that strive to obtain maximum value from the use of wireless devices, systems and services. Among other things spectrum management includes making rules (not only about radio operation but also the allocation and assignment of operating rights), ensuring that the rules are observed, and taking market structure into account where it affects the public interest. For the purpose here, the term interference resolution is defined to mean the elimination of interference between one radio operator and another, including cases where there is mutual interference. Interference resolution can be done by the operators themselves, or it may involve remediation and/or prosecution by the FCC. Interference resolution is thus a part of spectrum management.

The term enforcement has both broad and narrow meanings. In the broad meaning, it refers to interference resolution activities such as those undertaken by the FCC Enforcement Bureau. Those activities can be broken down into a variety of functions, such as monitoring – the observation of radio signals and detection, identification and location of interferers; adjudication – deciding whether observed interference is culpable; remediation, also called enforcement – terminating harmful interference by informal or formal action such as educating operators or imposing fines and seizing equipment. Enforcement is thus one of the tools for interference resolution and it can refer to wide range of activities or just remediation actions alone. To resolve this ambiguity, in the context of this study, enforcement is defined to mean the wide range of

[6] B. Obama. (2010, Jun. 28). *Presidential Memorandum: Unleashing the Wireless Broadband Revolution* [Online]. Available: https://www.whitehouse.gov/the-press-office/presidential-memorandum-unleashing-wireless-broadband-revolution

activities associated with interference resolution while remediation is defined to mean the much narrower set of education and punitive activities.

Activities associated with interference resolution are typically divided into two categories – *ex ante* and *ex post* (that is before and after the fact). *Ex ante*, in this context, refers to preventative measures taken in advance to eliminate or minimize subsequent incidents of radio interference. *Ex post* refers to actions taken after interference occurs. Examples of *ex ante* activity include making appropriate rules; authorizing equipment to ensure that devices operate in compliance with the rules or, say, educating the public about the negative consequences of buying and using an unapproved cellular radio jamming device. An example of an *ex post* measure would be a punitive, remediation action taken against the user of such a device once it had been put into service. The focus of the study proposed herein is on *ex post* systems and activities associated with interference detection, classification/identification, location, reporting, mitigating, and remediation.[7]

In Section 1 above, a distinction was made between non-malicious intentional interference and unintentional interference. An example of intentional interference without malicious intent would be an employer who uses an unauthorized device to jam cellular signals to prevent employees from making cellular calls or texting while engaging in hazardous activities. An example of unintentional interference would be interference inadvertently produced by an improperly aligned transmitting antenna lobe. The remaining category is malicious, intentional interference that conceivably could be produced by individual criminals, organized crime groups, foreign powers or non-state actors using unauthorized devices. While the focus of the study proposed herein is on non-malicious intentional interference and unintentional interference, the systems developed under the next generation systems architecture would obviously be of significant value in interference detection, classification/identification, location, reporting, mitigation, and remediation which is associated with both malicious intentional and non-malicious intentional interference.

Without resorting to formal technical definitions, the terms Electromagnetic Compatibility (EMC) and Electromagnetic Interference (EMI) are associated with unintended interference that may arise when electrical and electronic (i.e., telecommunications) equipment are operated in close proximity to each other. Under such circumstances the interference may not enter the receiving equipment through the antenna input jack but, for example, through other forms of coupling between the interference source and the receiver. A specific example would be electromagnetic energy that enters a receiver though a poorly shielded enclosure or via an associated power cord. EMC/EMI analyses and spectrum management are closely related but different disciplines and the focus of the study proposed herein it is on the latter rather than the former.

---

[7]Although the focus of the study is on *ex post* interference resolution activities, it is obvious (a) that there is a tradeoff between devoting limited resources to preventative activities versus punitive activities taken after-the-fact and (b) that much can be achieved by well-researched and well-grounded sharing studies conducted and acted upon in advance of deployment. The Federal Communications Commission's Technological Advisory Council recently developed a set of basic principles that should be considered in carrying out such decisions. See FCC Technological Advisory Council, Spectrum and Receiver Performance Working Group. (2015, Dec. 11). *Basic Principles for Assessing Compatibility of New Spectrum Allocations* [Online]. Available: https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting121015/Principles-White-Paper-Release-1.1.pdf

4. Specific Tasks/Key Activities

In carrying out the study, the performer shall execute the seven tasks described below. While the tasks are listed separately and sequentially, it is recognized that, realistically, all portions may be carried out in parallel and in an iterative fashion to produce the final deliverable – the next generation systems architecture for radio system interference resolution.

a. Document the Traditional Radio System Environment

The changing environment for interference resolution is illustrated by noting that, in the not too distant past, radio communications systems (i) typically operated in the analog mode with a very limited number of modulation methods or waveforms and used a single or limited number of (often) narrowband channels that were fixed or manually selected rather than dynamically assigned, (ii) utilized high power transmitters with high antenna sites that produced signals that were easy to detect and locate using relatively unsophisticated, manually operated spectrum monitoring and direction-finding systems, (iii) were typically noise limited rather than interference limited, (iv) were licensed by the Commission (or authorized by NTIA in the case of government systems), and regularly transmitted unique identifying information (e.g., call letters) in the clear and (v) transmitted the associated information content itself in the clear or in a form that was otherwise easily decipherable. Moreover, end-user devices had very limited processing, storage and display capabilities and had no means of ascertaining their location. Finally, unapproved transmitting devices designed for deliberate jamming were not widely available.

The purpose of this task is for the performer to document the traditional radio system environment including not only traditional communications systems but also other spectrum consuming systems such as radar and radio astronomy. This will provide a historical context for recent technological changes such as the migration from analog to digital modulation techniques in modern systems. In performing this task, the performer may rely upon the TAC White Paper dated May 29, 2014 entitled "Introduction to Interference Resolution, Enforcement and Radio Noise"[8] while conducting its own literature reviews and interviews or utilizing other research techniques.

b. Study and Document the Changes Occurring in the Radio Environment and the Challenges Associated with Them

In contrast to the traditional radio system environment described immediately above, the situation today is vastly different in nearly every respect. For example, many radio systems (i) increasingly operate in the digital mode using a myriad of complex waveforms that dynamically adapt to changing channel conditions while operating on multiple, dynamically

---

[8]D. N. Hatfield et al. (2014, Jun. 10). *Introduction to Interference Resolution, Enforcement and Radio Noise* [Online]. Available: https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting61014/InterferenceResolution-Enforcement-Radio-Noise-White-Paper.pdf. See also D. Hatfield. (2014, Mar. 31). *Keynote Remarks for WSRD SSG Workshop V: Understanding the Spectrum Environment: Data and Monitoring to Improve Spectrum Utilization* [Online]. Available: https://www.nitrd.gov/nitrdgroups/images/d/dd/Understanding_the_Spectrum_Environme_-_Hatfield_-_keynote_remarks.pdf

assigned broadband channels scattered over numerous bands that may be shared with other services on an active basis, (ii) often transmit at low power and low elevations from hundreds of antenna sites in order to provide the necessary capacity (through frequency reuse) to communicate successfully with millions of highly mobile end user devices consuming and producing a rapidly increasing amount of broadband information (iii) are typically interference-limited rather than noise-limited especially in congested suburban and urban areas (iv) are often unlicensed (e.g., in the case of Wi-Fi networks) or licensed by rule rather than on an individual basis and are not required to transmit unique identifiers (e.g., call letters or their equivalent) or communicate in the clear (e.g., without scrambling or encryption) (v) transmit the information content itself in "noise like" digital formats so that it is difficult to detect and to decipher and hence to classify or identify interfering signals for interference resolution purposes. Furthermore, because of the increased demand for spectrum capacity, widely deployed nomadic and mobile systems are moving higher up in frequency in the radio spectrum – e.g., above 3 GHz and even into millimeter wavelengths.

Individually and in combination, the characteristics of these modern wireless systems present significant challenges to the relatively unsophisticated, manually operated spectrum monitoring and direction-finding systems used in traditional interference resolution activities. The dynamic nature of the modern wireless systems, the normal variability associated with radio propagation conditions, and the increased mobility of end user devices results in interference being highly intermittent in terms of time, space and frequency; furthermore, the shorter ranges associated with the use of lower power and higher frequency bands makes spectrum monitoring and direction-finding problematic from a limited number of fixed and mobile locations. From an end-user (and service provider) perspective, the noise-like characteristics of aggregated intentional and unintentional interference from multiple sources may manifest themselves as sporadic decreases in capacity rather than as an outright, easily distinguishable disruption of service. The interference resolution challenges are further compounded by the wider availability of unapproved transmitting devices designed for deliberate jamming.

These challenges are elaborated upon at some length in the TAC "Introduction to Interference Resolution, Enforcement and Radio Noise" White Paper referenced earlier while some specific challenges, such as temporary transmitter or receiver intermodulation, are dealt with in a more recent TAC paper entitled "Basic Principles for Assessing Compatibility of New Spectrum Allocations."[9] The purpose of this task is for the performer to build upon these reports in order to create and document a more in-depth and comprehensive understanding of the interference resolution challenges that are created by densification and an increasingly dynamic shared spectrum environment. A clear, in-depth and comprehensive understanding of these challenges is essential to the development of the next generation systems architecture for radio system interference resolution that is the ultimate objective of the entire study.

c. <u>Identify, Analyze and Document Improved Capabilities for Detecting, Classifying/Identifying, Locating, Reporting, Mitigating, and Remediating Interference</u>

[9] G. Lapin et al. (2015, Dec. 11). *Basic Principles for Assessing Compatibility of New Spectrum Allocations* [Online]. Available: https://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting121015/Principles-White-Paper-Release-1.1.pdf

While the developments described immediately above present significant challenges to traditional methods used for interference resolution, going forward the same or related underlying technological advances that produced them also hold great promise in terms of increasing the speed, efficiency and efficacy of interference mitigation and avoidance techniques. To take a simple example, the technology that enables frequency agility that can create harmful and hard to locate transient interference can also be used by the victim of that interference to evade it by moving to another channel or even another band.

More broadly, the falling cost and increased performance of digital signal processing, the increasing capacity and falling cost of computer memory, and the development of increasingly powerful mathematical algorithms have facilitated the expansion of sophisticated systems for interference detection, classification/identification, location, reporting, mitigation, and remediation. Such modern systems can significantly outperform the relatively unsophisticated, manually operated spectrum monitoring and direction-finding systems used in traditional interference resolution activities of the past.

For example, individual analog spectrum monitoring systems were severely limited in terms of (a) the amount of information on the radio frequency environment that they could collect, analyze in real-time, and store for later analysis and (b) their ability to share their information and analyses in a cooperative fashion with other, similar systems. Modern digital systems, on the other hand, are not only capable of collecting, displaying and storing signal amplitude information but phase (timing) information over wide-swaths of spectrum as well. That is, the monitoring systems (e.g., vector signal analyzers) are able to capture, analyze and store essentially all of the raw – i.e., I/Q[10] – information in an "RF spectrum snapshot" of the radio environment at a location[11] and the wider availability of broadband communications facilities allows the aggregation and analyses of spectrum monitoring data from multiple locations.

Furthermore, the reduced size, weight, primary power requirements and development costs (e.g., through the use of Software Defined Radio – SDR – techniques) of these advanced monitoring devices facilitate their being carried or mounted on various physical platforms ranging from satellites, to aircraft, to drones/UAVs, to fixed, high antenna tower sites, to low towers or poles, to ground based vans or other moving vehicles, to transportable packages that can be left at fixed location on a temporary basis, and to hand carried portable units. Each of these evolving platforms or form factors has a potential role to play in developing the next generation system architecture for interference resolution.

For instance, aircraft mounted monitoring equipment can be (and is being) used to detect multi-channel signal leakage from cable television systems – leakage that may cause interference to over-the-air commercial and governmental radio services. It can also be used to verify the coverage of terrestrial (e.g., commercial) mobile radio services and to monitor background noise level changes over broad geographic areas. Spectrum monitoring equipment mounted on drones

---

[10] I/Q [(I)nphase / (Q)uadrature] data shows both the changes in magnitude (or amplitude) and phase angle of a sine wave.

[11] The collected information could be for one entire band or for one channel within a band and it could be for one or more antenna directions/sectors and polarity (e.g., horizontal or vertical).

can be used for similar purposes over smaller areas and in reacting to specific interference incidents. There are already a number of "spectrum observatories" operating from high, fixed antenna sites in multiple locations that are useful for general spectrum occupancy studies as well as arrays of low antenna sites that are being distributed around critical installations such as governmental facilities or major transportation hubs to protect the perimeter against interference intrusion on critical frequencies. Ground-based vans and SUVs have traditionally been used for spectrum monitoring purposes by the FCC, NTIA and other government agencies such as the FAA (as well as commercial service providers for drive testing), while portable units with direction-finding capability have been the mainstay for locating an interference source once its general location is known.

The TAC White Paper entitled "Introduction to Interference Resolution, Enforcement and Radio Noise" referenced earlier noted that the rapid growth in "intelligent" end user devices with greater signal processing power, expanded memory capacity and online connectivity into the Internet raises the possibility of using crowdsourcing as a way of improving interference resolution activities. The FCC is currently using crowdsourcing techniques to gather anonymous data from the smartphones of thousands of volunteers in order to better assess broadband performance nationwide.[12] The FCC Speed Test, as the app is known, could be expanded on a voluntary basis to include utilizing smartphones or more specialized devices to detect, store and report information on suspected interference on a near real-time basis if needed. The information collected from end user devices could be combined with other information gathered by the end user's service provider from within the associated network (e.g., information on dropped calls or interrupted data connections) to detect, locate, report and assist in determining the cause of intruding or harmful interference.

More sophisticated spectrum monitoring platforms and equipment can be used in three other important ways as well:

<u>First</u>, as noted before, the dynamic nature of modern wireless systems, the normal variability associated with radio propagation conditions, and the increased mobility of end user devices results in interference being highly variable in terms of time, space and frequency. Accordingly, long term, manned monitoring is inefficient and significant improvements in efficiency and effectiveness can potentially be obtained by engaging in automated monitoring and remote reporting from locations and in frequency ranges that are of special interest because of interference concerns. By using the information from the automated systems, efficiency and effectiveness can be improved by dispatching interference resolution personnel only at times when more is known about the characteristics of the interference.

The same type of monitoring approach can also be used to establish a baseline knowledge of the signals present in a given area and band of interest under normal, uncongested conditions. The monitoring system(s) can then be used to more readily and automatically detect, classify/identify, locate and report on any intruders under abnormal conditions. Note that this information may not necessarily come from a separate standalone monitoring system. It could also come from a

[12] For a description of the FCC's Measuring Broadband America program see *Mobile Broadband America* [Online] Available: https://www.fcc.gov/general/measuring-broadband-america

spectrum analyzer connected to an application specific receiver actually handling live communications traffic from, for example, one sector of a commercial mobile radio system antenna.

Second, and related, measurements made by more sophisticated spectrum monitoring platforms and equipment can be used not only in their normal role of detecting intentional and unintentional interference, but also to provide feedback to the system causing the interference to allow it to automatically adjust its operation to mitigate the interference. In engineering terms, this changes interference management among users in a shared spectrum environment from an open loop system to a closed loop system. Operating on a closed loop basis would allow the stations to be operated closer to each other in terms of frequency separation, transmitting times and spatial separation.

Take the latter, spatial separation, as an example. Radio propagation conditions along a path from an interfering transmitter's output to a victim receiver's input can vary significantly, depending upon a host of factors, including changes in atmospheric conditions and in natural and manmade clutter[13] along the path between the two. In the VHF and UHF regions of the spectrum, certain atmospheric conditions can cause a propagation phenomenon called "ducting" that can result in abnormally strong signals at certain times of the year over certain paths. In some regions of the spectrum, signal strengths (and hence the resulting interference) will vary as crop conditions or the condition of deciduous trees along the radio path change with the season. With a closed loop system, when changes in conditions produce interference the system producing the interference could be instructed to reduce power, change its antenna characteristics, or take other measures to mitigate the interference. Such near-real-time changes could produce significant gains in spectrum efficiency in bands with cooperative sharing arrangements.[14]

Third, I/Q information collected from one or more different sources can be used for *ex post* forensic analysis to determine the root causes of a particular interference incident. This would work in a similar way to how flight data recorders or "black boxes" are used to give investigators clues to the causes of accidents associated with commercial aviation. The results of the forensic analyses could be used not only for de-confliction and remediation purposes but also for developing *ex ante* rules and regulations to reduce the occurrence of such interference incidents in the future. For example, if the harmonics from transmitters operating in a particular service regularly cause interference to systems operated in harmonically related spectrum, the rules regarding the radiation of such spurious emissions could be adjusted accordingly through a normal notice and comment rulemaking proceeding at the FCC.

The paragraphs above provide an introduction to how the falling cost and increased performance of digital signal processing, the increasing capacity and falling cost of computer memory, the development of increasingly powerful mathematical algorithms, and related developments have

---

[13] In addition to terrain, manmade structures, trees, large bushes and other vegetation (or, more generally land uses/land cover or "clutter") can cause radio signals to weaken significantly as they travel from one location to another. The associated, incremental loss in signal strength is referred to as "clutter loss."

[14] This would be particularly true in situations where the spacing is based upon an *a priori* worst-case analysis intended to reduce *ex post* risk of interference or to allow the entity producing the interference to make *ex* post modifications to its system without going through protracted negotiations or regulatory proceedings.

increased the availability or potential availability of sophisticated systems for detecting, classifying/identifying, locating, reporting, mitigating and remediating sources of interference. The purpose of this task is for the performer to conduct a more comprehensive and in-depth study of these emerging systems. The primary objective of the task is not to gauge the ultimate technical and operational value of any particular system or collection of systems, but, rather, how their existence might inform or guide the development of the next generation systems architecture for radio system interference resolution that is the ultimate objective of the entire study.

d. Identify Current and Evolving Radio Spectrum Interference Resolution Requirements

The next generation interference resolution system must be architected in a way that supports the functionality necessary on an *ex post* basis to prevent or mitigate the effects of harmful interference on wireless systems. There are at least four complicating factors that must be considered in developing the architecture:

First, the effects of harmful interference can range from endangering or disrupting critical navigation and timing systems such as GPS/GNNS over a wide area to affecting only a handful of commercial end user devices operating in a limited area. A further complicating factor is that the same functionality (say interference detection) that is critical to preventing and mitigating specific instances of harmful interference is also useful in discovering areas, frequencies and/or times where interference is approaching but has not exceeded harmful levels thus allowing preventative steps to be taken in advance of actual harm. Or, even lower in priority, the same functionality can be used to find and document underutilized spectrum that might be a candidate for reallocating or sharing.

Second, as alluded to before, certain geographic areas (e.g., transportation hubs) and/or services (e.g., GPS) may have specialized systems dedicated to detecting, classifying/identifying, locating and reporting encroaching interference. Choosing a balance between using specialized versus more general purpose interference resolution systems is a fundamental one from a systems engineering and architectural standpoint as is the extent to which the two interact in a cooperative fashion with each other to reduce costs or improve performance.

Third, in certain shared spectrum bands, spectrum is (or will likely be) managed by a Spectrum Access System (SAS) on essentially a real-time basis. The details of these SAS systems will vary depending upon the characteristics and requirements of the sharing services/systems in different bands. The point here is not to describe the details of these evolving systems but simply to note that the SAS systems may have available to them certain information (e.g., information gleaned from spectrum sensing) that may be useful to the more general purpose interference resolution system, and that the general purpose system may be able to help the more specialized system if the latter is impacted by interference from systems that are not under its control.

Fourth, there is a need to distinguish between interference data that are collected principally for routine occupancy, mitigation and de-confliction purposes, for example, and interference data that are intended to be used in formal remediation proceedings that may lead to legal sanctions such as fines, cease-and-desist orders, forfeitures, equipment seizures and even criminal prosecution. Clearly interference data collected in the pursuit of formal remediation proceedings must be handled even more scrupulously and issues such as data integrity, chain of custody, privacy, security and provenance must be addressed. Data integrity, in this context, refers to maintaining and assuring the accuracy and consistency of data between the time when it is collected until it is used in an administrative or court proceeding. It is essential to ensuring that the data presented at the proceeding have not been tampered with or corrupted.[15]

These four complicating factors suggest very different requirements for the next generation interference resolution system. The purpose of this task is for the performer to gain a more in-depth and comprehensive understanding of these requirements by finding and analyzing more detailed information about both the specialized and general purpose systems from the FCC, NTIA, and other agencies. This shall include understanding the underlying mission requirements and environments that are being addressed as well as identifying and analyzing the associated functional requirements and design constraints. Similar to the fourth task described in Subparagraph 4.c., above, the primary objective of the task is not to judge the appropriateness of these itemized requirements but, rather, to determine how their existence might inform or guide the development of the next generation systems architecture for interference resolution that is the ultimate objective of the entire study.

e. Identify, Analyze and Document Privacy Issues Associated with the Development of the Next Generation Systems Architecture for Radio Spectrum Interference Resolution

Section 4.c above described sophisticated new and improved systems and platforms for detecting, classifying/identifying, locating and reporting interfering signals. These developments promise vast improvements compared to the relatively unsophisticated, manually operated spectrum monitoring and direction-finding systems traditionally used for interference resolution purposes. However, proposals for the wider use of some of these more sophisticated systems and platforms may raise new privacy issues, the resolution of which may influence or constrain the development and deployment of these advanced solutions.

The traditional monitoring systems used for interference resolution were largely based upon spectrum analyzer technology that measured the received power versus frequency over a frequency range determined the capabilities of the instrument. While these scalar measurements were and are useful in characterizing some aspects of the desired and undesired (interfering) signals, scalar measurements of received power versus frequency are inadequate in terms of handling modern broadband signals which may be intermittent or “bursty” in character and which are likely to use complex modulation schemes and waveforms. By themselves, instruments using scalar measurement are unable to extract the information content from a received signal and thus provide a degree of privacy for the generators of the desired and undesired signals.

[15] Information on interference incidents collected by private sector or non-governmental actors presents different issues than evidence collected by an entity like the FCC which is charged by federal statute with enforcement. Also, evidence collected by automated versus manual techniques may present special issues in terms of system requirements.

Given the increasingly wide variety of desired and undesired signals and unintended and incidental radiation that may be encountered in interference resolution activities today, increasingly sophisticated monitoring systems that include vector signal analyzers or real-time signal analyzers are evolving. These evolving systems can provide significant advantages in terms of detecting, classifying/identifying, locating and reporting on interference by being able to capture, store, and analyze on a real-time or forensic basis *all* of the raw (I/Q) information from a wide swath of spectrum in a given location and direction.[16] Coupled with modern SIGINT[17] capabilities, these increasingly sophisticated spectrum monitoring systems can be used to classify/identify interfering signals for interference resolution purposes but the same type of capabilities can also be used to provide the raw bit streams associated with the end user's voice, data, image or video traffic. This bit stream may include identifying information (e.g., the equivalent of call-letters) sent in the clear (or not), meta-data providing information on the content being carried including, perhaps, its source and destination, and the content itself which may or may not be encrypted.

Such techniques could be extremely valuable in terms of interference resolution by, for example, allowing the identification of the unique signature of particular interfering device or class of devices (say the power supply of a lamp fixture from a particular manufacturer) or, using the decoded meta-data, identification of the base station antenna sector from which interference is being received. But these potentially powerful benefits must be balanced against the possibility that, barring some form of constraints, the end user's voice, data, image or video content and sensitive meta-data associated with the content may be monitored and exposed. The implications of such a loss of privacy may be different depending upon whether the monitoring is being done by a private sector or public sector entity and whether the interference is merely a temporary annoyance at one extreme or intentional, malicious interference that presents an immediate threat to the safety of life and property and homeland security at the other extreme.[18]

The purpose of this task is for the performer to identify, analyze and document such privacy issues and the contexts in which they might arise. The objective of the task is not to make judgments about the proper balance between privacy and security, but, rather, to convey how privacy concerns might influence or constrain the development of the next generation systems architecture for interference resolution that is the objective of the entire study.

---

[16] Up until recently, the amount of I/Q information that could be stored and electronically transported was severely constrained. This limited the real-time bandwidth that could be recorded and how long the recording lasted. These practical constraints reduced potential threats to privacy but the falling cost of digital storage and broadband digital transport have significantly reduced these restrictions. For example, it is now possible to collect hours of I/Q information with a real-time bandwidth of 100s of MHz over a frequency range into the tens of GHz.

[17] SIGINT (signals intelligence) is information gained by the collection and analysis of the electronic signals and communications of a particular target.

[18] For an overview of legal and ethical issues associated with the collection of real Internet traffic see W. John et al., "Passive Internet Measurement: Overview and Guidelines based on Experiences," *Computer Comm.*, vol. 33, no. 5, pp. 533–550, Mar. 2010. (link to full text). For a focused article on the legal aspects of spectrum monitoring see P. Ohm et al., "Legal Issues Surrounding Monitoring During Network Research," *ICM '07 Proc. 7th ACM SIGCOMM Conf. on Internet Measurement*, San Diego, Calif., 2007, pp. 141–148.

f. <u>Identify, Analyze and Document Potential Cybersecurity Issues Associated with the Development of the Next Generation Systems Architecture for Radio Spectrum Interference Resolution</u>

The changes envisioned in moving from today's system for interference resolution to the next generation version that takes into account the profound changes in the RF environment described earlier will inevitably lead to increased (or at least significantly changed) exposure of the system to cybersecurity threats and vulnerabilities.[19] Elements that might be included in the next generation interference resolution architecture are SAS systems, specialized and general purpose monitoring systems operated by various entities, and a host of others. Considering these elements and some recent interference/remediation issues, a number of threats can be easily postulated. For example, the FCC maintains more than 40 specialized, publicly accessible data-bases several of which are essential or at least useful in interference resolution. These include data-bases associated with licensing, radio call signs, equipment authorization and antenna structures.

Consider the first, licensing. If monitoring reveals a signal of interest in a band, a threshold question is whether or not the station is licensed or authorized to operate there. If the license data-base is compromised, a response to a query by the operator of the monitoring equipment could indicate that the station is licensed or authorized to operate in the band when, in fact, it is not. A compromised call letter data-base could lead to similar results. In either licensed and unlicensed bands or services, interference may be produced by the operation of illegal, unapproved equipment or devices. This means that a field agent or other person investigating an interference incident may be misled if the equipment data-base has been compromised. Finally, the FCC's antenna structure registration data-base can be useful in locating potential sources of interference and gaining access to the antenna site if needed. A compromised data-base could impede this process. Similar threats are associated with data-bases (e.g., the Government Master File) operated by NTIA and individual federal agencies.

The purpose of this task is for the performer to (a) research and assess cybersecurity threats associated with the migration to the next generation systems architecture for interference resolution, (b) develop and document insights that will help guide and inform the development of the next generation systems architecture to be carried out in the next task, and (c) provide requirements on that architecture based upon the assessment and insights. In carrying out this task, the performer should take advantage of cyber risk management strategies work already done – or being done – in the communications area including the NIST's Cybersecurity Framework (ICF), the National Initiative for Cybersecurity Education (NICE), the FCC's Communications Security, Reliability and Interoperability Council (CSRIC), numerous activities of the Department of Homeland Security and more focused network security work being conducted by industry/academic groups such as the Wireless Innovation Forum.[20]

---

[19] For a useful taxonomy of communications jamming techniques that are associated with the widespread availability of SDR technology, see M. Lichtman et al., "A Communications Jamming Taxonomy," *IEEE Security & Privacy,* vol. 14, no. 1, pp. 47–54, Feb. 2016.

[20] For a substantial amount of well vetted information that is directly relevant to this task, see FCC Task Force on Optimal PSAP [Public Safety Answering Point] Architecture, Working Group 1, *Cybersecurity and Next Gen Systems: Optimal Approach to Cybersecurity for PSAPs* [Online]. Available: https://transition.fcc.gov/pshs/911/TFOPA/TFOPA_WG1_Cybersec_Next-Gen_Systems-042915.pdf

g. **<u>Develop the Next Generation Systems Architecture for Radio Spectrum Interference Resolution</u>**

The purpose of this final task is for the performer to develop the Next Generation System Architecture for Radio Spectrum Interference Resolution building upon the insights and analyses contained in the six previous tasks (a. – f.). In the first phase of this task, the performer will develop a high-level conceptual architecture and framework within which detailed design can take place. Upon review and agreement of the governing body overseeing the accomplishment of the work, the performer will develop the more detailed architecture by identifying and specifying the major hardware and software components that will comprise the system, the functions to be performed by each of those components, the interfaces among these components, and the associated protocols that allow the components to communicate with one another using the interfaces.[21]

It should be recognized that the details of the architecture will vary depending upon a host of factors, many of which have been touched upon earlier. The architecture will depend upon whether the band and adjacent bands in question are statically or dynamically shared and with whom (federal only, federal and non-federal, or non-federal only), whether they are unlicensed or licensed/authorized, and what constitutes harmful interference for each of the involved services. Further, it should be recognized that, while sophisticated Spectrum Access Systems that rely upon geo-location data-bases and/or spectrum sensing hold great promise in terms of facilitating interference resolution, they are still largely in their development phases and mostly untested at scale. This means that many systems critical to the safety of life and property and to homeland defense will not have the potential protection of these systems for several years, and, in the interim, they still must be protected from harmful interference in the face of the challenges such as densification and intentional jamming of the types described in the report cited in Footnote 20. Thus it is essential that the performer in developing the next generation systems architecture for interference resolution take into account the protection of existing systems that are important to not only to the nation's social and economic well-being, but also to the safety of life and property and homeland defense.

5. Period of Performance

TBD

6. Deliverables

TBD

7. Cost and Resources

TBD

[21]For perhaps the best explanation of the ideas surrounding systems architecting, see M. W. Maier and E. Rechtin, *The Art of Systems Architecting,* 3rd ed. Boca Raton, FL: CRC Press, 2009.