United States Senate
WASHINGTON, DC 20510

December 4, 2024

The Honorable Robert P. Storch
Inspector General
Department of Defense
4800 Mark Center Drive
Alexandria, VA 22350-1500

Dear Mr. Storch:

We write to request that you investigate the Department of Defense's (DOD) failure to secure its unclassified telephone communications from foreign espionage, risking serious harm to U.S. national security.

On November 13, 2024, the Federal Bureau of Investigation and the Cybersecurity and Infrastructure Security Agency publicly confirmed that Chinese-government hackers compromised "multiple telecommunications companies," and that the data stolen included "customer call records data" as well as "private communications of a limited number of individuals who are primarily involved in government or political activity." The press has reported that the surveillance targets included President-elect Trump, Vice President-elect Vance, and Senate Majority Leader Schumer. This successful espionage campaign should finally serve as a wake-up call to officials across the federal government who failed to shore up the government's communications security, despite repeated warnings from experts and Congress.

On May 8, 2024, the Navy finalized a new DOD-wide contract for unclassified commercial wireless devices and services for soldiers and civilian employees. The contract can be extended up to 9 additional years, with a potential value of $2.67 billion. The wireless companies selected under the Spiral 4 contract include AT&T, Verizon, and T-Mobile, which were reportedly breached by China as part of the recently revealed "Salt Typhoon" hack.

In the two attached whitepapers, which DOD sent to Congress in July 2024 and October 2024, DOD confirmed that its contracted carriers have significant cybersecurity problems and are vulnerable to foreign surveillance. While DOD indicated that it has mitigated some of the risks posed by adversaries exploiting some of the carriers' vulnerabilities through encryption technology, it has also confirmed that other surveillance threats, such as foreign governments' ability to track the location of specific phones, can only be mitigated by the wireless carriers. This national security threat was publicly identified by the Department of Homeland Security in 2017, yet DOD has seemingly failed to include requirements in the Spiral 4 contract that the carriers address these vulnerabilities and protect DOD personnel from foreign espionage. As DOD considers the renewal of Spiral 4 contracts, DOD should require findings from third-party audits or conduct its own cybersecurity audits. DOD has communicated to Congress that it has

been unable to review third-party audits commissioned by carriers included in Spiral 4, which provide important information regarding the resiliency of carriers against foreign espionage

DOD's continued use of unencrypted landline phones and platforms like Microsoft Teams undermines secure communication at DOD. Teams and certain other platforms utilized by DOD are not end-to-end encrypted by default, causing concerning gaps in security that could easily be mitigated. End-to-end encrypted voice, video, and text messaging tools such as Signal, WhatsApp, and FaceTime better protect communications in the event that the company that offers the service is hacked. Despite the widespread availability of secure alternatives, agencies instead continue to use unencrypted phone lines and insecure communications platforms.

Some DOD components have begun to pilot, on a limited basis, a potentially more secure superior communications platform, known as Matrix, which is end-to-end encrypted by default, interoperable, not controlled by any one company, and widely used by multiple NATO allies. For example, the attached presentation, provided to Congress in July, describes the Navy's successful use of Matrix, including on 23 ships. While we commend DOD for piloting such secure, interoperable communications technology, its use remains the exception; insecure, proprietary tools remain far more widespread within DOD and the federal government generally. The widespread adoption of insecure, proprietary tools is the direct result of DOD leadership failing to require the use of default end-to-end encryption, a cybersecurity best practice, as well as a failure to prioritize communications security when evaluating different communications platforms.

DOD has defended its continued use of unencrypted landline phones, which it described as "acceptable from a risk-management perspective" in the attached whitepaper, dated August 29, 2024. DOD told Congress that it assessed "that there are no 'unnecessary' risks posed by such use" of landline phones. DOD further defended the practice as "balanc[ing] acceptable risk with operational requirements" and stated that "prohibiting [telephone] collaboration would have a significant negative effect on DOD's world-wide, real-time mission, and is unnecessary to protect unclassified communication." Less than three months after DOD provided that whitepaper to Congress, the press reported the Salt Typhoon hack of U.S. telecommunications companies, and several other federal agencies reportedly directed their employees to stop communicating via phone lines.

DOD's failure to secure its unclassified voice, video, and text communications with end-to-end encryption technology has left it needlessly vulnerable to foreign espionage. Moreover, although DOD is among the largest buyers of wireless telephone service in the United States, it has failed to use its purchasing power to require cyber defenses and accountability from wireless carriers. The responsibility for such failures cannot and should not be pinned on low-level procurement officials, but rather, reflects a failure by senior DOD leadership to prioritize cybersecurity, and communications security in particular. We urge you to investigate DOD's failure to secure its communications, and to recommend the changes in policy necessary to protect DOD communications from foreign adversaries. Further, DOD's Spiral 4 contracts are actually one-

year contracts, which the government can renew up to 9 more years at its discretion. We urge you to consider whether DOD should decline to renew these contracts and instead renegotiate with the contracted wireless carriers, to require them to adopt meaningful cyber defenses against surveillance threats, and if requested, to share their third-party cybersecurity audits with DOD.

Sincerely,

Ron Wyden
United States Senator

Eric S. Schmitt
United States Senator

Appendix A:
July 2024 Info Paper

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

(U) Info Paper: Signaling System 7 (SS7)

(U) Background: Senator Wyden's Senior Technologist/Senior Adviser for Privacy and Cybersecurity requested that the Department of Defense (DoD) answer twelve questions regarding the DoD Chief Information Officer (CIO) Controlled Unclassified Information SS7 Information Paper that the Department provided to the Senator's office in December 2023, as well as two additional questions about the DoD Wireless Services Contracts Spiral 4 vehicle.

(U) Questions and DoD Responses

1. In April 2017, DHS published a thorough report on mobile security threats, which included the following three statements on page 77. Can you please let me know if DoD agrees or disagrees with each of these assertions by DHS in its 2017 report:
   a. "[DHS] believes that all U.S. carriers are vulnerable to [SS7 and Diameter] exploits, resulting in risks to national security, the economy, and the Federal Government's ability to reliably execute national essential functions."
   b. "[DHS] believes SS7 and Diameter vulnerabilities can be exploited by criminals, terrorists, and nation-state actors/foreign intelligence organizations."
   c. "[DHS] believes many organizations appear to be sharing or selling expertise and services that could be used to spy on Americans."

   Answer: The Department of Defense (DoD) agrees with the SS7/Diameter assertions listed on page 77 in the DHS report, "Study on Mobile Device Security," April 2017.

2. In April 2023, Sen. Wyden sent a letter to CISA and NSA regarding the security of FirstNet, which is used by DoD. That letter revealed that in a Feb 2022 briefing on SS7 security, CISA's subject matter expert told Senator Wyden's staff that they had "no confidence in the security of FirstNet, in large part because they have not seen the results of any cybersecurity audits conducted against this government-only network." Does DoD share the concern of the CISA subject matter expert regarding the security of FirstNet? Has DoD seen the details (the scope, the results, and whether discovered issues have been mitigated) related to FirstNet's SS7 and Diameter security audits, and if not, what is the basis for DoD's confidence in the security of FirstNet?

   Answer: Questions about the security of FirstNet should be addressed directly to the FirstNet Authority and the Department of Commerce.

3. In that same April 2023 letter, Sen. Wyden asked CISA for a copy of a report CISA commissioned titled "U.S. telecommunications insecurity 2022." CISA refused Senator

Wyden's request for a copy of the unclassified report, but permitted Senator Wyden's staff to come to CISA's office to read the report. The report contains alarming details about SS7-related surveillance activities involving U.S. telecommunications networks. Has DoD received a copy of this report? If not, has DoD requested a copy of the report? If DoD has not requested a copy of this report, please do so, and provide us with your response to the troubling allegations in the report.

Answer: Yes, DoD has received the report referenced above. Assessments of the allegations contained in the report should be addressed directly to the Cybersecurity and Infrastructure Security Agency (CISA).

4. The Dec 2023 information paper you provided to Senator Wyden's office indicates that "All DoD Providers commission third-party audits and penetration testing." Has DoD reviewed the details (the scope, the results, and whether discovered issues have been mitigated) related to these audits and penetration testing? If not, what is the basis for DoD's confidence in the security of these networks, as the audits could have discovered serious security problems that have not been mitigated.

   Answer: No, DoD has not reviewed the details. However, all DoD Providers informed us that they follow the Communications Security, Reliability, and Interoperability Council (CSRIC) recommendations and Global System for Mobile Communications Association's (GSMA) guidelines by commissioning third-party audits and penetration testing, while actively tracking industry updates for new threats to cellular networks on an ongoing basis. Questions regarding the specifics of third-party audits should be addressed directly to the providers (i.e. carriers).

5. Has DoD performed or commissioned its own SS7 and Diameter audits into DoD Providers? If not, please explain why.

   Answer: No, DoD was informed by the providers that they routinely conduct third-party audits and penetration testing and have implemented the Global System for Mobile Communications Association's (GSMA) best practices for SS7 and Diameter signaling security as well as the corresponding Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council (CSRIC) requirements.

6. How confident is DoD that the security controls used by DoD Providers are sufficient to protect DoD personnel using DoD-provided mobile devices from SS7 and Diameter enabled surveillance by foreign adversaries?

   Answer: There are limited protections against SS7/Diameter weaknesses within DOD's Telecommunication Providers (i.e., carriers), therefore DoD managed mobile solutions encrypt data in transit to protect against passive collection.

7. Does DoD require DoD Providers to disable, by default, roaming and all reject SS7 and Diameter traffic for DoD users from Russia, China, and other high-risk countries and foreign global titles known to originate malicious SS7 and Diameter traffic? If not, why not?

Answer: No, Industry standard practice established the routing policy for mobile global titles based on the Mobile Country Code (MCC) and the Mobile Network Code (MNC) portion of the individual International Mobile Subscriber Identity (IMSI) (i.e. DoD user). Routing message traffic between networks based on the granularity of the full IMSI as a global title is not typically supported nor practical.

8. In September 2017, DHS personnel gave a FOUO presentation on SS7 security threats at an event open to U.S. government personnel. Sen. Wyden's staff attended that event. The attached photo shows a slide from that DHS presentation identifying the "primary countries reportedly using telecom assets of other nations to exploit U.S. subscribers." Those countries, according to the DHS presentation, are Russia, China, Israel and Iran. The slide also identifies a number of countries in Africa, Central/South America, and Europe, the Middle East, and Africa whose telecom assets have been by those previously listed countries used to "attack US subscribers." Does DoD disagree with the information presented by DHS in that presentation, indicating that these foreign governments are using SS7 to target U.S. users, and that these SS7 attack are being routed through 3rd country networks?

   Answer: DoD is not in a position to render an assessment without access to the underlying data that informed this presentation.

9. Is DoD aware of any incidents in 2022 or 2023 in which DoD personnel, whether located in the U.S. or outside the U.S, were surveilled through SS7 and Diameter enabled technologies? If the answer is none, how confident is DoD that this means that DoD personnel were not in fact subject to such surveillance. If the answer is yes, how many DoD personnel were surveilled via such means in 2023 and 2023?

   Answer: Requires a classified response.

10. Are there security measures that carriers in other countries are taking to protect against SS7 and Diameter surveillance that, if employed by DoD Providers, would better protect DoD personnel? If yes, please identify these security measures and any steps taken by DoD to request that DoD Providers implement these measures.

    Answer: DoD is currently unaware of any other risk mitigations that countries have undertaken to protect against SS7 and Diameter vulnerabilities.

11. Has DoD received any reports of SS7 and Diameter-related surveillance targeting DoD personnel stationed in Guam and Diego Garcia? If yes, what steps, if any, has DoD taken to confirm and mitigate these threats?

    Answer: Requires a classified response.

12. Are there any domestic wireless providers that offer superior protections against SS7 and Diameter-enabled surveillance than the security provided by DoD Providers? Please describe the specific steps taken by DoD to determine whether the answer to this question is yes or no, and how confident DoD is in its answer.

Answer: Questions to provide a comparative assessment of protections against SS7 and Diameter-enabled surveillance should be addressed directly to the providers.

13. Why did DoD CIO not provide NAVSUP with requirements for Spiral 4 related to SS7 surveillance, interconnection security, and roaming threats from adversarial countries?

    Answer: The Spiral 4 performance work statement (PWS) requires National Information Assurance Partnership (NIAP) and Defense Information Systems Agency (DISA) standards per paragraph 6.8 Network Approved Device Requirements which mandates: "All mobile devices shall meet all requirements of the NIAP Mobile Device Fundamentals V3.3, or its successor, and must be DISA certified for connection to the Department of Defense Information Network (DoDIN)." Spiral 4 PWS paragraph 6.9 NIAP states: "As NIAP and DISA standards change, the Contract may be modified to include these evolved capabilities of the devices and Service Plans offered. Contractors shall conform with the required NIAP and DISA standards or be off ramped in accordance with PWS Section 7.8.b."

    The Spiral 4 PWS also added a new requirement, which was not included in Spiral 3, per paragraph 6.10 Security Breach/Cyber Incident, to report "when any third party has received unauthorized access to any Contractor operational networks or storages for any data associated with Contractor furnished devices and services…"

    This requirement will provide DoD with increased awareness of security incidents.

14. Whether NSA was invited to provide input on the minimum cybersecurity standards for the Spiral 4 contract, and if not, why."

    Answer: DoD Spiral 4 PWS requires NIAP and DISA standards per paragraph 6.8 and 6.9.

Appendix B:
October 2024 Info Paper

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

Info Paper: Signaling System 7 (SS7)

Questions and DoD Responses

1. *In the whitepaper DoD provided to Senator Wyden, DoD confirmed that it believes that all U.S. carriers are vulnerable to SS7/Diameter surveillance (Q1) and that the carriers DoD has contracted with have limited protections in place against SS7/Diameter surveillance (Q6). DoD further confirmed that it has not conducted its own security audits of the carriers' networks (Q5), nor has it reviewed the results of the 3rd party audits commissioned by the carriers (Q4).*

   a. *Has DoD asked the carriers for copies of the results of their 3rd party audits? If not, why?*

      Answer: Yes, the DoD has asked the carriers for copies of the results of their third-party audits and were informed that they are considered attorney-client privileged information.

   b. *Why did DoD not require that approved Spiral 4 vendors submit the results of their security audits, including SS7 and Diameter audits, to DoD for review?*

      Answer: DoD has requested the then Spiral 3 now Spiral 4 vendors for copies of the results of their third-party audits.

   c. *Is DoD confident that DoD-contracted carriers fixed all of the security problems discovered during their most recent 3rd party audits and implemented all corrective actions recommended by the auditors? If not, why?*

      Answer: DoD has asked the carriers for copies of the results of their third-party audits and were informed that they are considered attorney-client privileged information.

   d. *Does DoD have the legal authority to conduct cybersecurity audits, including for SS7/Diameter vulnerabilities, of the services that DoD-contracted carriers provide?*

      Answer: DoD is reviewing the Spiral 3 and 4 performance work statements (PWS) and coordinating with General Council and Contract Authority to determine if the

Department has the legal authority to conduct cybersecurity audits of contracted carriers.

2. *In the whitepaper DoD provided to Senator Wyden, DoD stated in response to question 6 that due to the SS7/Diameter vulnerabilities in DoD-contracted carriers networks, it utilizes encryption to mitigate the risks of passive surveillance by adversaries. Please confirm that such encryption only protects against interception of internet data transmitted to and from those mobile devices (web browsing, email, etc.), but does not protect against location tracking performed using SS7/Diameter. What mitigations, if any, has DoD employed against adversaries' location tracking using SS7/Diameter, and if DoD has not employed any mitigations against adversaries' ability to track DoD personnel's locations exploiting SS7/Diameter, please explain why.*

   Answer: DoD cannot fully answer these questions at the unclassified level.

3. *In the whitepaper DoD provided to Senator Wyden, DoD stated in response to question 10 that "DoD is currently unaware of any other risk mitigations that countries have undertaken to protect against SS7 and Diameter vulnerabilities." The Secretary of Defense was CC'd on a February 2024 letter from Senator Wyden to President Biden, related to SS7 and Diameter threats, which is available here [1]. Page 2, paragraph 5 of that letter references the United Kingdom's Telecommunications Security Code of Practice, a 149-page document that requires wireless carriers take specific technical measures to protect their networks from malicious cyber activities, which include mitigations against SS7 and Diameter threats. That UK government document can be accessed here [2]. The UK government has also conducted multiple rounds of SS7/Diameter penetration tests of UK carriers, as described here [3]. According to the UK government, those audits discovered vulnerabilities that were "quite serious." The Ukrainian government has also reportedly taken a number of steps to harden their networks against SS7 attacks Russian hacks, which are described in this series of blog posts [4]. Please confirm that DoD was not, prior to this email, aware of these actions taken by these close allies to secure their telecom networks from SS7/Diameter threats. Now that you have this information, please review it, and confirm whether DoD assesses that any of the security measures adopted by the UK and Ukraine, if adopted by DoD-contracted carriers, would make it harder for adversaries to surveil DoD personnel.*

   Answer: The DoD was aware of the United Kingdom's Department for Digital, Culture, Media and Sport, "Telecommunication Security Code of Practice," December 2022 but not of any other countries' mitigations undertaken.

   In reviewing the SS7 section in the National Cyber Security Centre (NCSC) Active Cyber Defence – Third Year [3] (pg. 41) document, while DoD values security assessments, DoD does not have the capability to perform similar assessments of DoD contracted carriers. Additionally, while DoD applauds security measures taken by the UK and Ukraine, we do not yet have great confidence that requiring similar measures in DoD contracted carriers would have significant impact on our adversaries' SS7/Diameter exploitation capabilities.

   Requests to provide a comparative assessment of protections against SS7 and Diameter-

enabled surveillance should be addressed directly to the providers.

4. *In the whitepaper DoD provided to Senator Wyden, in response to question 13, asking why DoD did not require SS7 surveillance defenses as a condition of the multi-billion Spiral 4 contract for wireless service, DoD cited paragraph 6.8 in the contract, relate to security requirements imposed by DoD for mobile devices. Since SS7/Diameter surveillance exploits vulnerabilities in the carriers' networks and does not involve any contact with the target's phone, please explain how the requirements cited by DoD related to device security will mitigate SS7/Diameter attacks. DoD also said that these measures will provide DoD with increased awareness of security incidents. Please explain how these measures will provide DoD with increased visibility into SS7/Diameter surveillance.*

   Answer: DoD cannot fully answer this question at the unclassified level.

5. *Please identify the parts of the NIAP and DISA standards that DoD-contracted carriers must meet, cited by DoD in response to question 14, that require DoD-contracted carriers to adopt specific technical defenses against SS7/Diameter surveillance and please specify the steps that DoD has taken to assess the effectiveness of these measures.*

   Answer: The DoD Spiral 4 performance work statement (PWS) requires NIAP and DISA standards per paragraph 6.8 and 6.9 that ensures E2EE to protect CUI data, but the remaining SS7/Diameter vulnerabilities must be addressed by the carriers.

Appendix C

Response to [redacted] Senator Wyden

RFI Response regarding DoD use of insecure call in #s for Zoom/Teams/WebEx and the use of approved positive disconnect devices.

1. **Question: From the perspective of DoD, when employed by a DoD employee in a SCIF/SAPF, communicating unclassified information to other, non-DoD persons not in a SCIF/SAPF, which method of communication is more vulnerable to surveillance by adversaries: (1) Unencrypted Plain Old Telephone Service (POTS) calls to a conference call number or (2) Zoom/Teams/WebEx, using a CNSS/TSG-approved disconnect device?**

   Response: From our perspective, the two methods you describe are both acceptable from a risk management perspective for transmitting (discussing) non-public unclassified information; however, both are vulnerable with respect to the communications intentionally being transmitted (discussed). For example:

   - Unencrypted POTS can potentially be intercepted by an adversary via the commercial phone system;

   - Many of the unclassified collaboration tools available on the market do not employ properly implemented end-to-end encryption, allowing an adversary to intercept the audio, just as with a POTS call. A DoD review of collaboration tools during the COVID-19 pandemic (the most recent review) showed that fewer than half employed properly implemented end-to-end-encryption.

   - Properly-implemented end-to-end encryption provides computer audio using a CNSS/TSG-approved disconnect a level of protection against the audio being intercepted in transmission. Even when using such encryption, the use of a full computer system (typically Microsoft Windows, given that the question involves individuals a SCIF/SAPF) significantly increases the attack surface, as compared with a desktop telephone unit, and offers an adversary the potential ability to collect the audio from a compromised computer system.

2. **Question: What steps has DoD taken to alert DoD personnel of the unnecessary risks posed by using POTS dial in #s for group calls, and of the security benefits of using encrypted computer audio, where available? If DoD has not taken any such steps to warn DoD personnel, why?**

   Response: DoD utilizes an intelligence-informed risk management process when assessing capabilities such as these. At this time DoD assesses that there are no "unnecessary" risks posed by such use and therefore has not issued any specific alerts on the use of POTS dial ins. Consistent with federal-wide policy and DoD's risk management (vs. risk elimination) approach, DoD permits the use of both models for unclassified collaboration.

In these instances, only unclassified information may be communicated over either method, thus the compromise of the information being discussed does not lead to damage to national security. This reduction in consequence allows DoD to balance acceptable risk with operational requirements.

NSA frequently issues publicly-available cybersecurity advisories and guidance (not alerts) – including guidance on telework best practices and on selecting and safely using collaboration services.

3. **Question: Why has DoD not prohibited POTS dial in functionality for DoD-organized unclassified group calls given the widespread availability of more-secure, encrypted unclassified communications tools that use computer audio?**

   Response: Computer audio is not as widespread as may be perceived, and even when available, does not always have properly implemented end-to-end encryption. Prohibiting POTS-based collaboration would have a significant negative effect on DoD's world-wide, real-time mission, and is unnecessary to protect unclassified communication.

4. **Question: Why has DoD not required DoD-personnel joining unclassified group calls organized by other organizations to utilize encrypted computer audio whenever it is an option?**

   Response: See previous answers.

Appendix D

DoN Brief to the Senate Finance Committee Fellow and Sen. Wyden Staff

July 2024

Matrix Application

Department of the Navy

PEO C4I

MCSC

SDO

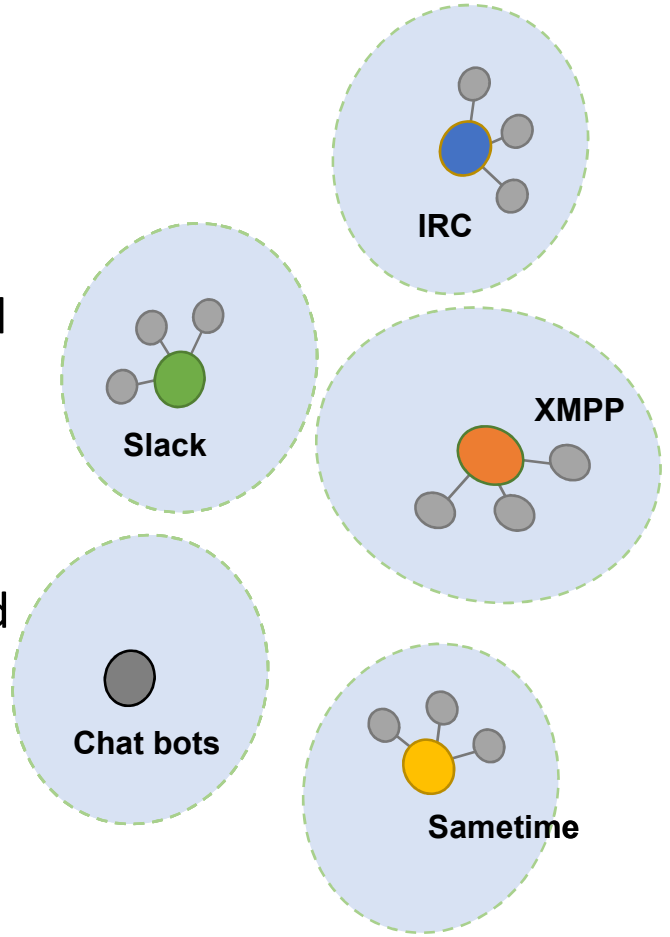
Navy Tactical Chat Today

- Shore based servers. Clients must have stable network connection to shore network centers for any functionality
- Multiple separate protocols with no cross talk/connections
  - IRC client(Mako) and servers(Bahamut)
  - XMPP clients and servers
  - Coalition networks use Sametime and/or XMPP
- Centralized hub and spoke architectures have limited COOP
- IRC is not secure in transit, and has weak if

any authentication

- XMPP is fragmented over different specifications and solutions are not always interoperable
  - Limited in functionality supported by protocol, and uses/requires more bandwidth

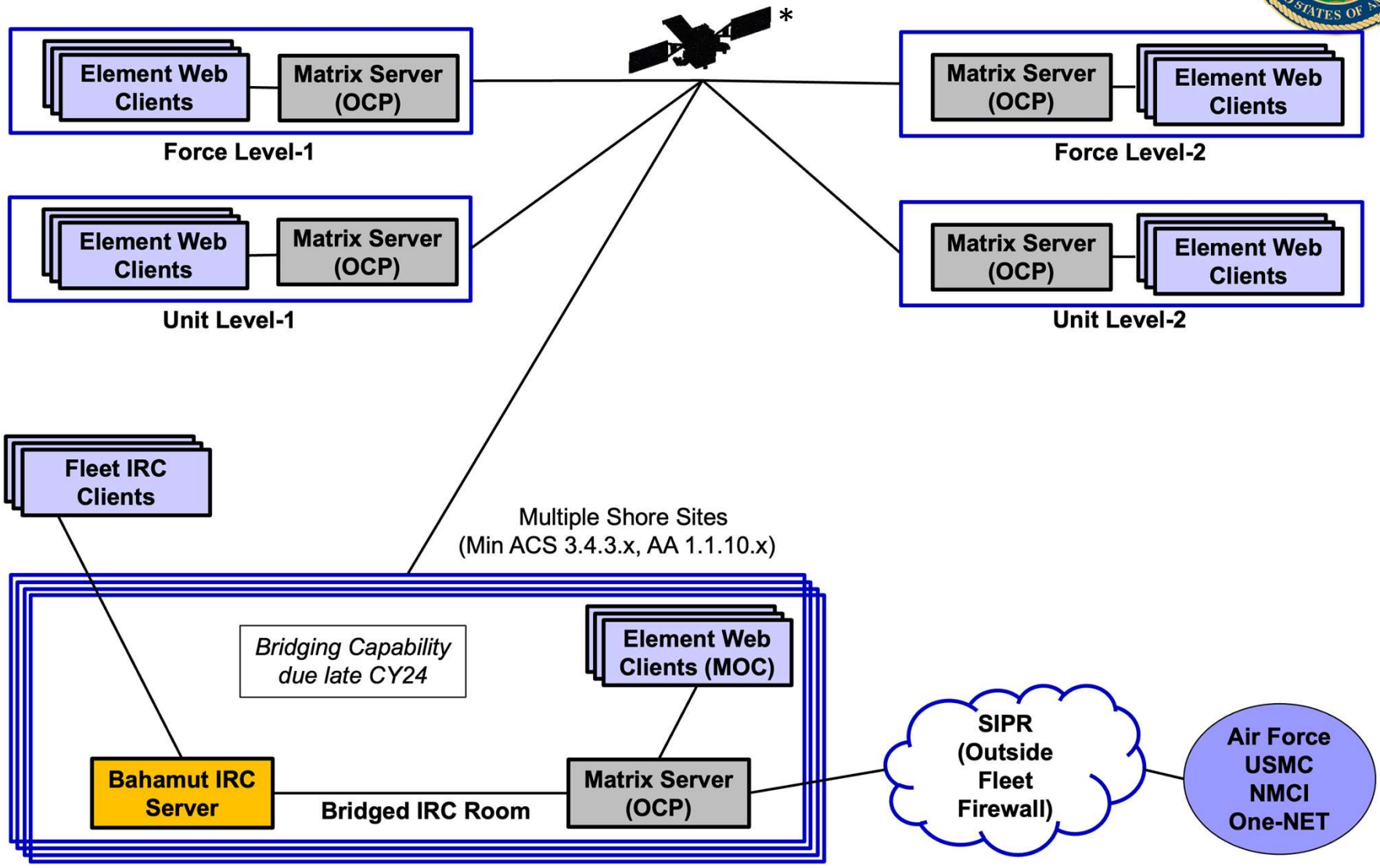
Silos of Protocols



What is the Matrix protocol?

- Open-source protocol for decentralized real-time communications (Chat, VoIP, IoT)
- Offers end to end strong encryption, in transit, at rest, per user certs/keys used for strong data separation, direct antivirus support
- Single monolithic specification insuring compatibility between Matrix applications
- Synchronizes conversation history (as opposed to passing messages)
- HTTP+JSON make up the baseline API
- Bridges many other communication protocols together
- Features
  - Decentralized conversation history
  - Cryptographic integrity of conversations
  - Multi-device synced history
  - Rich text messages
  - Extensible message formats
  - Encrypted file transfer
  - Typing notifications
  - Read receipts
  - Decentralized room administration
  - Avatars
  - Synchronized read markers
  - Synchronized message counts
  - Server-side push notifications
  - Server-side search
  - VoIP and Video calling & conferencing

Tactical Chat (using matrix protocol)



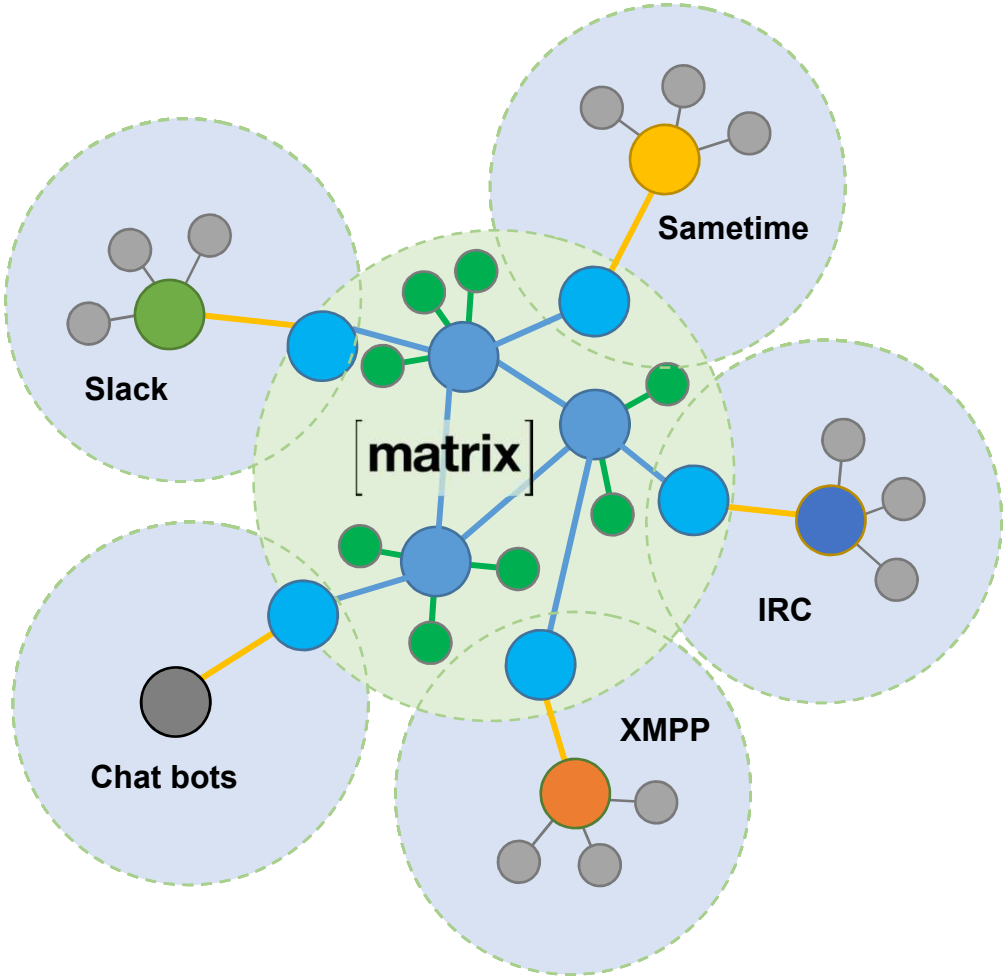
* - Note while SATCOM is shown any TCP/IP networking path can be used

Matrix Architecture

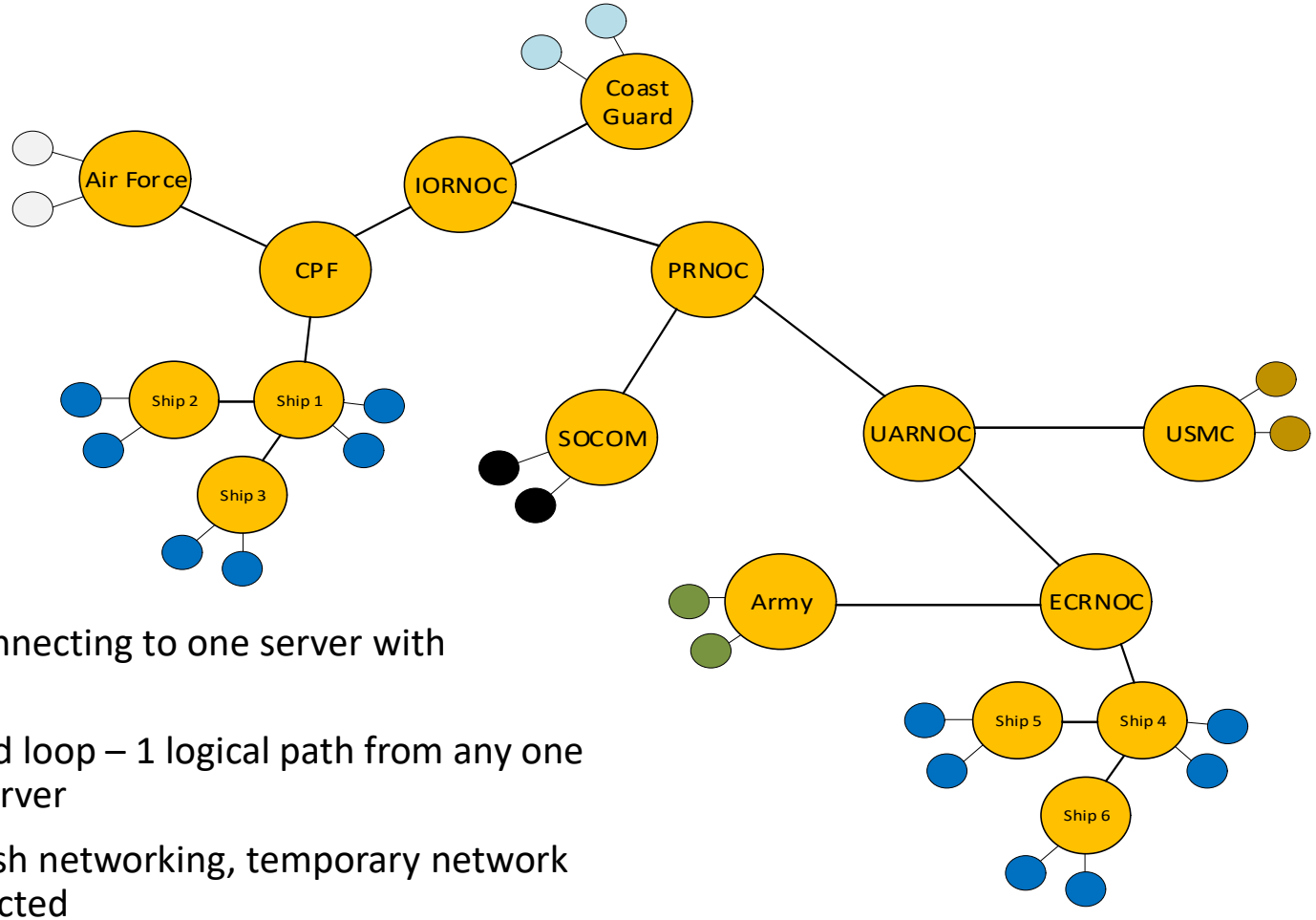
Clients

Home Servers

Application Servers



Federated Architecture



- Individual clients connecting to one server with federated rooms
- Never forms a closed loop – 1 logical path from any one server to another server
- Works well with mesh networking, temporary network segmentations expected
- Any TCP/IP network path supporting secure connections can be used

Tactical Chat (Matrix)

Capability Short Description

- Matrix is an open standard protocol, with multiple open-source software implementations for interoperable, decentralized, real-time comms over any IP network
  - The reference implementation server is called Synapse. Synapse is open-source software, available on GitHub.
  - The web client is called Element, others are available
- Afloat the combined solution is hosted on CANES Agile Core Services OpenShift Container Platform (OCP), as a containerized application, and clients connect using a standard CANES web browser.
- Ashore the combined solution is hosted on specific localized servers at key nodes, with the addition in Q4FY24 of a production IL6 cloud environment. Any SIPR client can connect to the localized nodes or IL6 cloud environment.
- Matrix servers (Synapse) will connect to other Matrix servers in a mesh network with no single point of failure.
- The clients and servers are DoD PKI enabled, users must have a physical SIPR token to login to any client/server and an admin token to perform the installation and setup.

FY24/25 Deployments and Milestones

- Currently installed on 23 afloat units and 3 shore sites
- Built, scanned, and deployed through Overmatch Software Armory, continual cyber grade “A”
- FY25 Milestones:
  - Utilization of Overmatch Production cloud environment (DEC24)
  - Admin GUI/Console and IRC/XMPP bridge (DEC24)
  - Tiled client supporting multiple chatrooms
  - Continued deployments and operational support