Advisory Committee on Commercial Remote Sensing (ACCRES)

Wednesday, August 24, 2022 9:00 AM – 3:00 PM

Meeting Attendees

Committee

- **Mr. Gil Klinger** (Committee Chair), President, Gil Klinger Consulting LLC
- **Ms. Krystal Azelton,** Secure World Foundation *(not present)*
- **Dr. Asha Balakrishnan,** Science & Technology Policy Institute (STPI)
- **Mr. Payam Banazadeh,** Capella Space
- **Mr. Gregory Black,** Gregory E Black LLC
- **Dr. Chris Boshuizen,** Data Collective Venture Capital *(not present)*
- **Mr. Kyle Foster,** Leidos
- **Mr. Tony Frazier,** Maxar Technologies
- **Dr. Henry Hertzfeld,** Space Policy Institute
- **Mr. Eric Ingram,** SCOUT Inc.
- **Mr. Prasad Komma,** Microsoft Azure
- **Mr. Tony Lin,** DLA Piper
- **Mr. Todd Master,** Umbra
- **Ms. Pamela Meredith,** KMA Zuckert LLC
- **Mr. Kevin D. Pomfret**, Centre for Spatial Law and Policy
- **Mr. Tommy Sanford,** Commercial Spaceflight Federation
- **Mr. Robert H. Schingler Jr.**, Planet Labs

Special Guests

- **Ms. Erin Miller**, Space Information Sharing and Analysis Center (ISAC)
- **Mr. Adam Dickinson**, Federal Bureau of Investigation (FBI)
- **Ms. Holly Shorrock**, Department of Homeland Services (DHS)

Department of Commerce/National Oceanic and Atmospheric Administration

- **Dr. Stephen Volz**, Assistant Administrator for Satellite and Information Services, NOAA
- **Mr. Alan Robinson**, Acting Director, Commercial Remote Sensing Regulatory Affairs and Committee Acting Designated Federal Official (DFO), NOAA
- **Mr. Glenn Tallia,** Chief, Weather, Satellite and Research Section, NOAA General Counsel

Meeting Minutes

ACCRES Welcome — **Alan Robinson**

Tashaun Pierre introduced Mr. Alan Robinson. Mr. Robinson welcomed all committee members and guests. He informed everyone that the previous director, Ms. Tahara Dawkins, left the office in January 2022 to take a position with the National Space Council. Mr. Robinson stated that he is the acting office Director until a permanent director is identified. He then introduced Dr. Stephen Volz.

Greeting & Introduction of Committee Chair — **Dr. Stephen Volz, NESDIS AA**

Dr. Stephen Volz introduced all of the new ACCRES members. He stated that NOAA will be looking for new members and a new ACCRES chairman following this meeting. He provided a quick background of himself (Dr. Volz). He reiterated the focus of today's meeting being cyber security and informed everyone that CRSRA has published (new) Guidance Circulars (GC's) on our website. He introduced the next speaker, Mr. Gil Klinger.

Opening Remarks & Introduction of Committee **Gil Klinger, Chair**

Mr. Gil Klinger, ACCRES Chairman: Mr. Klinger thanked all committee members and, as outgoing chair, looks forward to being able to help out in the future. He stated that cybersecurity is increasingly important for any commercial remote sensing company, especially when working with the government. He informed everyone this will be a working session and to be ready to have a conversation. Mr. Klinger noted that NSPD 27 will have its 20th birthday in April and that he would like to see this policy updated.

Mr. Klinger conducted a committee roll call and introduced all current ACCRES members, and then turned the meeting over to Mr. Robinson.

Mr. Robinson introduced the next speaker, Ms. Erin Miller.

Cyber Security Awareness **Erin Miller, ISAC**

Ms. Erin Miller is the VP and Executive Director of the Space Information Sharing and Analysis Center (Space ISAC) and on the Board of CyberSat and CyberLEO.

Ms. Miller: Greetings: I have a 2-part presentation - Part 1 - Background on the Space ISAC and - Part 2 - Showing how we view cybersecurity and what to do about it.

The Space ISAC (S-ISAC) was formed to facilitate global coordination/communication on cybersecurity. The basis for the Space ISAC was a federal study stating the need to break down information sharing silos, and the need for more cyber threat information to reach the commercial industry.

There are 30 ISACs (all but the Space ISAC represent critical infrastructure sectors). Only one is for space. All share critical (threat) intelligence and vulnerabilities. The Space ISAC is a Public Private Partnership (PPP). Member companies are organized by sectors. There are also international partners - allied space agencies (ESA, JAXA, DLR) etc. The board is composed of a broad array of members from FFRDCs (Federally Funded Research and Development Centers), universities, and industry.

The National Cyber Center (NCC) hosts the space ISAC in Colorado Springs. The Space ISAC (will) share threat data and vulnerability information through a (secure) Watch Center which will open next year. The Space ISAC takes a multi-decade approach to protecting space, and is not political. It is operationally focused to solve problems for operators across the globe in a high trust environment. Ms. Miller made note of the founding board member companies and their makeup.

Protecting space (systems) helps protect humanity.

One current key focus: zero trust architecture to ground stations as a service

ISAC Structure and meeting tempo: Annual summits - task forces drive topics. Quarterly meetings including at SmallSat 2022, where the discussion was around using blockchain to increase security, also AI/ML attack vectors. The ISAC is organized into multiple Communities of Interest (COI). The Work Force Community of Interest (WFCOI) plans to map our competencies for cyber for space.

Working groups (WG):

Analysis WG - 1st line of defense for the watch center, members receive monthly threat briefings.

Supply Chain WG - securing supply chains, needs more members/partners with global supply chain insight.

Member portal up since Feb 2021 with daily, weekly and monthly reports. It is a threat information portal and actionable threat/intel briefings. The S-ISAC has deliverable products - OSCAR, Secure space daily summary, etc. Over 500 daily reports delivered to-date.

S-ISAC partnered with ODNI to read-in members of the space industry with need-to-know for a classified briefing on Ukraine (in March 2022).

The **Watch Center** is located in CO Springs. It is not operational yet - but will reach IOC in Q1 2023, allowing the tracking of adversary actor's ground and space activities to increase space security. The Watch Center will;

- Converge on Cyber and physical threats
- Fuse data from disparate sources
- Leverage Azure Machine Learning & Data Science products to provide analytics/events of interest to the community
- Display visualizations for analysts
- Offer Space ISAC analysts from public and private sector access

Space threat taxonomy - by space, link, ground segments;

The Space ISAC placed a Request- for-Info (RFI) in July to ask the space/member community what they thought about space/cyber risks, threats, and vulnerabilities.

Detailed answers: (see slides)

Summary: Most threats to the remote sensing space sector are threats to commercial systems (not civil), and cover the gamut of RF threats, orbital debris, cost of encryption, cyber hacking of the space/ground segments and loss of space segment control. This includes attacks that impact the CRS payload as well as other parts of the satellite system (common to all space systems).

ISAC offered to send a report on RFI responses as a draft to this Committee in the future (**the report is not completed yet**).

The responses to the RFI) noted a number of concerns about Radio Frequency (RF) Electromagnetic Interference (EMI) (**Threat scenario 1**). Specific threat information on RF attacks will be displayed using tools at the watch center. The plan is to be able to display such attacks visually.

Satellite Maneuvering (**Threat Scenario 2**) satellite maneuvers will be tracked and members will be alerted of significant maneuvers.

Nation-State Actor Threats (**Threat Scenario 3**) The Watch Center will leverage information from the Microsoft (MS) Threat Intelligence Center (MSTIC) and provide relevant data to members.

Attacks to space link: (**RFI Threat scenario 4**)

The Watch Center and Cyber Vulnerability Lab will open in Q1 2023.

Question: Mr. Robinson-With encryption are assets still vulnerable?

Answer: Miller-Have not checked this yet, but planning to do so. We currently only have input from Subject Matter Experts (theoretical).

Question: Tony Lin: Are the labels specifically relevant to CRS? The noted risks seem to apply to any type of satellite versus (only) remote sensing systems/payloads.

Answer: Miller-Yes, although some apply to all space vehicles/systems. Will have her team test if there are threats specifically to CRS that do NOT affect other parts of the Space Community.

Question: Kyle Foster: Great briefing. Given the overlap between civil and CRS, are you finding best practices specific to the CRS sector?

Answer: Miller: Mitigation (technique) depends on the type of attack.

Question: Kyle Foster: In the Identification of vulnerabilities, is the S-ISAC considering the quality and age of the (space or ground) hardware as part of the risk/ threats?

Answer: Miller-Has not come up in risk assessments, but has been considered. Tabletop exercises are designed to compare legacy architecture to new and cloud based(ground) systems.

Question: Tony Fraser: How is the S-ISAC working with other organizations - government etc?

Answer: Miller- The S-ISAC is where unclassified info sharing will occur, there is some overlap with the DoD's Commercial Integration Cell (CIC) but the S-ISAC mission/role is broader than the CIC. The S-ISAC would like to partner with the CIC to leverage threat and vulnerability information and do bi-directional info sharing (CIC has 7000 members).

Cyber Security for Remote Sensing **Adam Dickinson, FBI / Holly Shorrock, DHS**

Mr. Robinson Introduced Adam Dickinson and Holly Shorrock.

Adam Dickinson: Greetings. Glad to be following Erin and building on her presentation. Both my and Holly's agencies (FBI & DHS) work to counter cyber threats. We will start with a broad overview of the space cyber landscape and review common threats to this sector. In the second half of our presentation we will look specifically at CRS and SATCOM and what the threats mean to critical infrastructure applications.

Introduction of terms (refer to slides). Noted the (large) economic value contributed by remote sensing. Major terms: Space System, SATCOM, Remote Sensing, and Imagery.

Commercial GEOINT - remote sensed data (source NGA for this slide) is used for Imagery, Map features, Analytics (and services). The USG buys imagery from commercial sources.

How CRS data is used for Information and Knowledge services. (see slide)

How attacks occur within a CRS space system.

Holly Shorrock: Attacks occur to one of three distinct segments – the Ground, Space or the RF link. Some recent publications have also referred to a 4th: the "User segment". All segments are vulnerable; however, the ground segment is the most vulnerable. An attack on the space system can have spillover effects far beyond the space system itself. They can persist for weeks or months, creating doubts in the public and users minds about the reliability of the provider and the space sector itself, as well as incurring large financial burdens for recovery.

Ukraine attack - Electronic attacks (launched in addition to the cyber-attack) gave Russia military advantage but also affected transportation, energy, aviation, etc., infrastructure far outside Ukraine.

Common electronic attacks: GNSS (GPS) spoofing and (RF link or RF sensor) jamming. Both are easy and inexpensive, Russia has used these techniques many times. The use of these in Ukraine caused planes to be grounded and diverted, an effect lasting for up to a week.

It was previously thought that space segments were not vulnerable, as well as commercial systems. Not so.

Other spillover effects on space: The sanctions on Russia as a result of Ukraine caused satellite launches to be canceled, as well as research projects and other deals. This has delayed RS and SATCOM constellations (i.e. OneWeb). The attack by Russia on KASAT confirms that the ground is the most vulnerable part of the network, but not the only portion.

General cyber threats and vulnerabilities: Space is subject to a variety of enduring threats. Cyber actors use a variety of attacks including supply chain-based attacks. Robust cyber security must be part of every space system. Many hardware and software components are shared between systems, hence the compromise of one component could have devastating effects across the space sector (Example - the solar winds attack).

Bad actors have monitored US systems for compromised meteorological data that originated outside the US.

Insider threats (ITs) are costly (and common). IT attacks caused $38M per incident in the US last year. Examples include, employees, individuals who act on their own, individuals acting on behalf of others, and those having various motivations.

Lax physical security is a compounding factor. Insider threat security often falls between different departments and therefore may not be well addressed since responsibilities are not clearly defined.

Dickinson: **Impacts of cyber-attacks**: 3 categories - availability, confidentiality, data integrity.

SATCOM vs remote sensing - see slide. SATCOM (user) terminals are particularly vulnerable pathways for a cyber-attack. A high impact attack occurs when the remote device has high access to the internet. Remote sensing data is widely used across all 16 critical infrastructure sectors, making them vulnerable to attacks on CRS.

Application Specific Impacts

Dickinson: CRS is used in the **energy sector** for a variety of uses; planning, risk management, resource availability (inventory), and movement - maritime shipping and pipeline transit.

SATCOM is (also) used in the energy sector for a variety of purposes, including moving data around and remote control of equipment (this function was targeted by the STUXNET virus). Attacks could affect exposure of data, damage to equipment, and risk to human life.

Shorrock: **Agriculture sector**: this is very large: 2.1 million farms, 935k restaurants, etc., as much as 20% of the nation's economic output. Same uses and vulnerabilities as the energy sector for both SATCOM and CRS risks. Cyber Security of these sectors is complex but can be mitigated.

Conclusion:

SATCOM vulnerabilities impact multiple sectors

- Affect all parts of energy supply chain
- Affect entire agriculture value chain

Potential for compounding, negative impacts to human safety

SATCOM cybersecurity dependent on non-human factors

- Environmental Disruptions
- Energy Supply to Systems
- Shifts in Interconnectedness

Reporting: Report cyber incidents to the FBI field office. Consult the CISA website for cyber threat information.

CISA: https://us-cert.cisa.gov/report

FBI: fbi.gov/contact-us/field-offices or 855-292-3937

Questions: To be submitted to the CRSRA office

Cybersecurity and Space Support Systems **Robert Bunge, NOAA**

Mr. Alan Robinson introduced Mr. Robert Bunge.

Mr. Bunge: Greetings and thanks. My presentation/information might seem redundant compared to the previous briefings but I will provide some new observations including from a NOAA perspective.

The threats: NOAA is attacked thousands of times daily. This should be common knowledge. Many attacks are "script kiddies" looking for basic security "holes" - unpatched software, spear phishing email, etc.

Some of the threat vectors: Traditional network attacks: unpatched servers/network gear, website vulnerabilities, email/chat and communication servers, weak/poor encryption, misconfiguration, trust relationships. Other sources (see slide).

Supply chain: A new vector for consideration is data flows from "partners" (ingested data). How do we manage the integrity of the data flow? Part of the answer is for NOAA to monitor (political) changes in the source country/government that might reduce data trust.

Challenges in the space environment: NOAA has many legacy systems. These can become hard to protect as the software /hardware ages, or as the vendor undergoes business changes. Also, NOAA has mission critical systems that cannot be taken down for maintenance. Patching these systems takes time, but new regulations (and threats) reduce the time allowed for such work.

Multiple threat vectors: in addition to those mentioned, malware can be delivered on USB devices, and there are emerging problems with "Trusted" partner/vendor relations- how do we manage their security posture?

NOAA employs "Risk Based Mgt". There are many frameworks available for this (incl. what NOAA uses - FISMA/NIST 800.53). These employ multiple levels of officials to manage security posture and status of each system (see slide).

Space/Environmental data: A key aspect of the (science) community is there is never enough data and there is a desire to keep old systems operating as long as possible for continuity of observations/measurements- the goal is to handle the challenge of keeping such systems up-to-date with cyber protection.

Most NOAA systems are used to generate/feed data into operational (weather) models used to generate forecasts for DoD and commercial customers and protect agriculture, transportation, etc. sectors. This data has safety of life/property implications.

NOAA buys data and must ensure the integrity of this data. NOAA must understand these data flows, have backups or solutions in case the data flow is stopped, "poisoned", or otherwise disrupted.

Applying Cyber Framework to Satellite Ground systems: notes that there is now specific guidance in NIST 8401 (released April 2022)

Question: Kyle Foster- Another new Cybersecurity Guidance Circular was released last week. Have you reviewed the circular and does it meet the needs of the moment?

Answer: Mr. Bunge has not yet had a chance to read/review the document. He will follow up with Mr. Alan Robinson.

LUNCH

CRSRA Update **Alan Robinson**

Mr. Alan Robinson presented CRSRA updates

- Licensing Statistics
  - 98 active licenses
  - On track to meet or exceed licensing actions in CY21
  - Average of 24 days to issue licenses in CY22 to date, 50% reduction since implementation of new regulations
- Compliance Statistics
  - 762 licensed GS, 418 active, 178 inspected
  - 44 sites inspected since July 2021 - 8 investigations
  - Inspections allow CRSRA to assist and support licensees, strengthening their security posture, as well as identifying any compliance shortfalls
  - Priorities for inspections include Tier 2 and Tier 3 Mission Control Centers (MCCs), and those requested by our Interagency partners

Committee Work Session on Guidance Circular **Alan Robinson**

Mr. Alan Robinson outlined the purpose of the Committee's working session.

- Purpose of Working Session
  - Review and discuss CRSRA Guidance Circulars (GC)
    - Suggestions for new topics
    - Proposed edits to existing GCs
- Definition of GC
  - CRSRA interpretation of Regulations
  - Living documents, do not have the force of law

- Published on CRSRA website
- Current GCs
  - 7 published, 2 in development
  - US Person/Operating
    - Definition of “operate”, “person”, “U.S. person”
  - Affiliates/Subsidiaries
    - Definition of “subsidiaries” and “affiliates”
  - RGIQE
    - Definition of equation for comparing SAR systems
  - Mission Assurance
    - Definition of “mission assurance” and methodology for determining exemption
  - Data Submission (Tier 3 Evaluation)
    - Outlines process for evaluation of Tier 3 data related to TLC clock-start
  - Cybersecurity
    - Outlines CRSRA view of required and recommended cybersecurity practices
  - Ground Station Classification (in development)
    - Definition of ground station types, uses, and licensing requirements
  - Instrument Classification and Tiering (in development)
    - Definition of instrument types, uses, and licensing requirements using FWHM
- Direction for ACCRES Working Discussion
  - What other topics should CRSRA consider for new/additional GCs?
  - Are there any suggestions for changes to existing GCs?

Question: Tony Lin - How can we better communicate the existence of the GCs to licensees? All licenses should be informed, not just those directly affected. One other thought, can you provide the dates for document updates and version numbers on each GC?

Answer: We have communicated directly to impacted licensees and we will note that broader distribution is recommended. CRSRA agrees that we need to increase awareness. Publishing dates and version numbers can be added and will be considered.

Question: Tony Frazier: Regarding the cybersecurity GC, the “required” NIST standard noted as aimed at Federal systems, and we believe it should be NIST 800-171 standard instead.

Answer: The requirement was selected based on NRO/NGA requirements that may be applied to Tier 3 systems in the Temporary Conditions. CRS systems with propulsion should apply NIST standards for encryption and other controls.

Question: Henry Hertzfeld - Regarding the Mission Assurance GC, the adjudication of cameras that observe the spacecraft is based on the amount of time used for these purposes. Can you please clarify the paragraph?

Answer: We are trying to be consistent in our approach to adjudicating the exemption, so we are basing it on the capability and the “primary” intended use. We will look carefully at the text and consider changes.

Question: Kyle Foster - GC’s do not have the force and effect of law.

Answer: The Licensee is bound by the license conditions.

Anje Hall - For example, if a licensee did not follow the guidance in the cybersecurity GC which led to a non-compliance and or violation of a license requirement, they could be found negligent.

Question: Tony Lin - The Cyber GC is very long (51 pages) and different from the others. Should it emphasize that it is only for guidance? It does not succinctly clarify the rules, like the other published Guidance Circulars, such as the GC that works through the nuances of what is a "US person". The implications of the cybersecurity recommendations in the GC are not clear.

Kyle Foster: inclined to agree.

Question: Tony Lin - A good idea for a new GC would be one discussing Ground Station inspections and addressing questions like how long the process takes and how licensees should prepare?

Answer: We will add guidance for onsite inspections to the list.

Question: Pam Meredith - Can you provide more guidance for ground station operators? Today, ground station operators are taking on more control (uplinking commands) of systems, so may have "control" of the system as defined by the GC on "operator". The FAA has similar guidance and lists a number of factors that they consider.

Answer: We are seeing more of this kind of control by contractors, but the determination we make is "who has the ultimate authority" to make decisions and the relationship between those entities is what we are looking at.

Question: Kyle Foster - Should there be language in the Affiliates/Subsidiaries GC about (how to) transfer a license in the event of a corporate acquisition?

Answer: Additional guidance does not seem to be needed, as there is no such thing as a license transfer.

Glenn Tallia: It seems to be addressed in the regulations, but we can look and see if we can make it clearer.

Question: Tony Lin - Looking at the existing GC's where are the GC topics going and who is developing the documents? Is it possible (for industry) to give input prior to publication? The majority of the existing GC's seem fine, but I have concerns about the cybersecurity GC due to its length and complexity.

Answer: Glenn Tallia - these are living documents that can be revised at any time. These are intended to address repeated issues that we've seen under the new regulations over the past two years.

Alan Robinson - CRSRA and General Counsel noted consistent themes that we observed in responses to the new regulations. I am inclined to stay with the living documents approach with input after publication.

Question: Tony Lin - most read as common questions that CRSRA has received, except the Cybersecurity GC. It doesn't seem like CRSRA was applying direct expertise to develop it.

Answer: CRSRA consulted with external expertise to develop the cybersecurity Guidance Circular.

Question: Tony Frazier - Cyber GC reads like a guideline rather than a FAQ. Adding an executive summary might improve the usability of the document.

Answer: Glenn Tallia - This is CRSRA's attempt to be helpful in defining "industry standards" and provide general guidance.

Alan Robinson - Data protection requirements were removed from the new Regulations.

Question: Danielle Pineres - With regard to Tier 3 Data submission, in the list of actions on page 5, it might be helpful to clarify what happens if a license modification is required. What happens when the data you submit is the same as data from other sources?

Answer: It is based on your licensed capability - If the data you provide is better than your licensed capability, you will need to submit a modification. If the data you provide is worse than your licensed capability, you would need to submit a modification (if you wish to) lower your Tier. CRSRA can automatically re-tier when it becomes aware that new data is available, or a licensee may request to be re-tiered. We will look at adding a note about re-tiering.

Question: If the data is already available from other sources, should that result in automatic re-tiering and cessation of temporary conditions without the need for a licensee to request a modification?

Answer: CRSRA will look at this idea.

Question: Danielle Pineres - CRS systems will improve revisit rates over time, including foreign systems and available data. How do we get re-tiered when our own revisit rate is exceeded if it is our revisit rate that causes us to be classified Tier 3 with temporary conditions?

Answer: Send CRSRA evidence of revisit rates by foreign systems. If found to be accurate, CRSRA may re-tier or remove certain conditions.

Question: Danielle Pineres - is it possible for proliferated Low Earth Orbit constellation license holders to request changes to TLCs unrelated to revisit prior to achieving the revist capability?

Answer: This seems logical and we will consider it internally.

Question: Danielle Pineres - Can Mission Assurance be expanded to include on-board SSA capabilities/sensors for the tracking and observation of nearby ARSOs (that could present a threat to our mission)?

Answer: Probably not, but will be considered. Related to NEI conditions.

Question: Todd Master - With regard to RGIQE, how are determinations made for foreign capability? Adding language to the GC might be useful. Our concern is that foreign systems seem to provide better data than is indicated in the current Tiering process and we want to make sure that actual performance is being considered.

Answer: Alan Robinson - We will take a look.

Question/Comment: Todd Master - clarity on how revisit rates are determined would be useful. **Q**: Danielle Pineres - In the Cyber GC there is a lot of focus on NIST encryption standards, but there are also good encryption standards from industry that might be appropriate.

Answer: CRSRA will consider.

Question: Pam Meredith - If a US company sets up a foreign subsidiary operating outside of the US, who needs to have a license? Does the US parent company need a license? Can additional examples be created in the GC?

Answer: There are a number of scenarios of corporate relationships that would need to be examined on a case by case basis.

Question: Tony Lin - Mission Assurance - I'm reading this as though there has been a change to the policy on Mission Assurance. Can prior decisions be revisited?

Answer: Glenn Tallia - the GC reflects our current thinking and interpretation. There is no reason that prior decisions cannot be reconsidered, or prior Initial Contact Forms resubmitted. Alan Robinson - we would welcome the opportunity to re-evaluate existing licenses. The Mission Assurance GC was written with this in mind.

Suggestion: Tony Lin - FCC has a process whereby the public submit questions (knowledge database) and the staff answer them, while pointing to existing guidance and regulations.

Response: Good suggestion. We do have a FAQ on the website and we don't have a large enough staff at this time to support such an effort.

CLOSING REMARKS

- CRSRA welcomes follow-up remarks/suggestions from ACCRES/public
- No follow-on Working Groups will be established

Public Comments **Alan Robinson**

Anne Cortez

- **Q**: After ICF submitted and "license required" - is it possible that no license may be ultimately required after application is submitted?
  - ANS: Yes - it is possible
- **Q**: If a US company uses a foreign subsidiary to get a radio license, do they need a US imaging license?
  - ANS: It can be complicated - corporate relationships require case-by-case analysis

Closing Remark & Next ACCRES Discussion **Alan Robinson**

Alan Robinson closed the meeting with proposals for the next meeting

- Recent polling suggested overwhelming support for virtual meetings among ACCRES members
- Advanced planning would allow adjusted timing for East/West Coasts
- Proposal to meet toward the end of February
  - CRSRA will communicate with committee

Meeting Adjourned 3:00 pm EDT