WaTech
Washington Technology Solutions

SIEC WASHINGTON

State Interoperability Executive Committee

June 13, 2023

1:30 pm – 3:30 pm

WaTech
Washington Technology Solutions

SIEC WASHINGTON

Agenda

- Welcome & Introduction
  - Review agenda
  - Member News and Information Roundtable
  - **Approval** of April 11 meeting minutes
- National Interagency Fire Center Capabilities – Kirk Maskalick, Jose Lopez
- SAW Group Updates – Anton Damm
- Cybersecurity Grant Updates – Zack Hudgins
- Legislative Session Updates – Bill Kehoe
- SCIP Goals Workshop – Bill Kehoe
- Good of the Order / Public Comment

WaTech
Washington Technology Solutions

Review April 11 Minutes

National Interagency Fire Center

National Interagency Incident Communications Division

(NIICD)

DISCUSSION POINTS

- NIICD/NIRSC
- Incident Support
- Equipment
- Frequencies
- Team Pre-Orders
- Type III Support
- Technical Training
- Communications Duty Officer (CDO)
- GACC Reps/Questions

National Incident Radio Support Cache (NIRSC)

NIIICD/NIRSC's mission is to provide portable emergency communications, technical training, and airborne remote sensing imagery services in a professional, prompt and customer-oriented manner, while optimizing resources and minimizing risks.

- Rework & Supply
- Maintenance
- Avionics
- National Infrared Operations
- Communications Operations
- Engineering & Development
- Technical Training
- Communications Duty Officer (CDO)

NIICD/NIRSC Incident Support

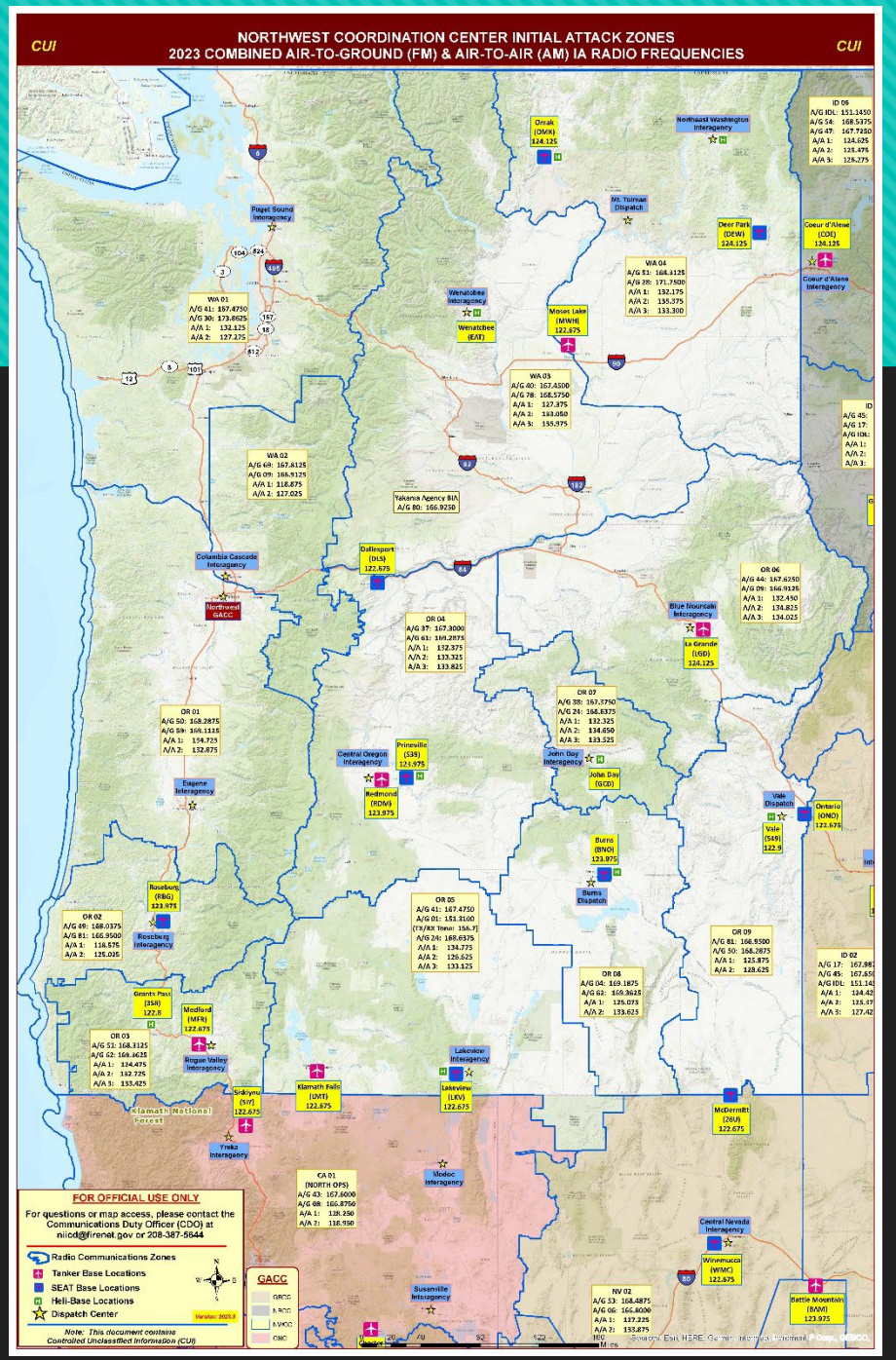
- Mostly Supports Wildland Fires
  - 200-300 Fires (average)
  - 120-150 Starter Systems (average)
- Special Operations
  - Military Exercises
  - Law Enforcement
  - Drug Interdiction
- Hurricanes
- Other Disasters
  - Oils Spills
  - 9/11
  - Shuttle Columbia Recovery
  - Floods
  - Earthquakes (USAR)
  - Oklahoma City
- Special Events
  - 2002 Winter Olympics
  - 1995 Summer Olympics
  - Wright Brothers Centennial
  - Political Conventions
  - 4th of July Celebrations
  - Wildlife Management Roundups
- International Response
  - Office of Foreign Disaster Assistance (OFDA)
  - Disaster Assistance Response Teams (DART)
  - US Forest Assistance Support Program (DASP)
  - DOI/BLM – International Programs

NIICD/NIRSC Radio Equipment

- Handheld Radios
  - VHF 136-174 Range (P25 Compliant)
  - UHF 400-420 Range (P25 Compliant)
  - 12,500 Total
    - RELM DPHx
    - RELM BKR5000
    - RELM KNG2
    - MIDLAND
    - Motorola
- Portable Repeaters
  - 180 VHF (P25 Compliant)
  - 98 UHF (P25 Compliant)
    - Codan/Daniels Electronics
- Misc Equipment
  - Satellite Phone Kits (Iridium)
  - Aircraft Links
  - Air Attack/Military Aviation Kits
  - Solar Panel Kits
  - Battery Kits
  - Remotes
- Price of Equipment
  - No Daily Cost
  - Refurbish Cost
  - Damaged/Missing
  - Shipping Cost

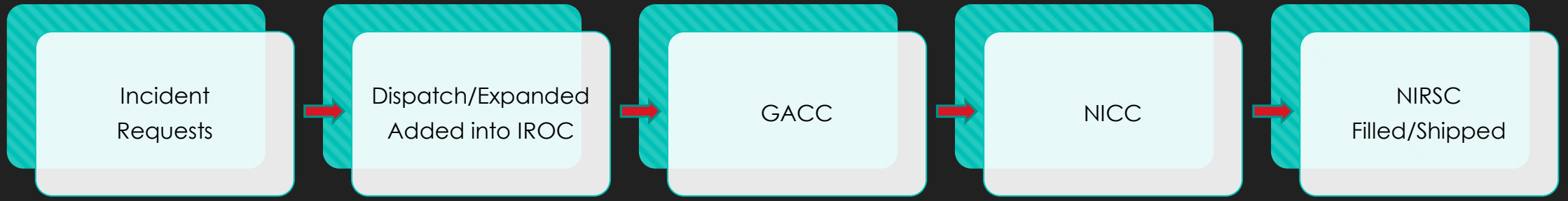
NIICD/NIRSC Frequencies

- USDA/DOI (Not Available Nation Wide)
  - 23 VHF FM
  - 27 UHF FM
- NTIA (Not Available Nation Wide)
  - 20 VHF FM
  - 14 UHF FM
- AFTRCC
  - 5 A/A AM
- FAA
  - A/A AM Incident Specific
  - Engineered by the FAA
  - Tanker Bases/SEAT Bases
- Initial Attack Zones
  - 105 IA Zones Nationally
    - A/A AM
    - A/G FM
  - FAA AM Frequency
- Temp Incident Frequencies
  - DOI/USDA
  - USPS/FEMA/DHS
  - Justice/Treasury Dept.
  - State
  - 30-day Authorization



NIRSC Ordering Process

Equipment



Frequencies

NIRSC Type III Support

- NWCG does not require a qualified COMT or COML for ordering Radio handhelds and misc. equipment

- NWCG and NIRSC requires a qualified COMT or COML for ordering 4390's and repeaters.
  - 4390 – Starter System
  - 4312 – VHF Command Repeater Kit
  - 4248 – UHF Logistics Repeater Kit
  - 4370 – Aircraft Link Kit

- The more type III incidents NIRSC supports the less that is available for Type I and Type II incidents
  - Frequencies are not an infinite resource

NIRSC Technical Training

- NWCG Incident Communications Support Training
  - S-258 Incident Communication Technician (COMT)
    - Offered yearly throughout the country
  - S-358 Incident Communications Unit Leader (COML)
    - Offered yearly throughout the country depending on demand
  - Communications Coordinator (COMC)
- NIRSC Training Coordinator
  - Kirk Maskalick
  - kirk.maskalick@usda.gov

Communications Duty Officer (CDO)

National level coordination and assignments for incident frequencies and equipment is the responsibility of the National Interagency Incident Communications Division (NIICD) and is managed by the Communications Duty Officer (CDO).

- Maintains the capability to respond to any type of natural or human caused disaster, law enforcement and special events.
  - Equipment
  - Frequencies
  - Personnel
- Available 24/7
- 208-387-5644
- niicd@firenet.gov

- CDO Coordinator:
  - Kimberly Albracht
  - Kimberly.Albracht@usda.gov

NIICD/NIRSC GACC Representatives

Questions??????

- NRCC, RMCC, AICC
  - Jose M. Lopez
  - (208) 387-5858
  - jose.lopez2@usda.gov
  - USDA, Forest Service Telecommunications Specialist
- GBCC, ONCC, OSCC, SWCC
  - Albert Karnowski
  - (208) 387-5826
  - akarnowski@blm.gov
  - DOI, Bureau of Land Management Telecommunications Specialist
- EACC, SACC, NWCC
  - Kirk Maskalick
  - (208) 387-5861
  - kirk.maskalick@usda.gov
  - USDA, Forest Service Telecommunications Specialist
- NIFC Communications Duty Officer (CDO)
  - (208) 387-5644
  - niicd@firenet.gov

WaTech
Washington Technology Solutions

SAW Group Updates

WaTech
Washington Technology Solutions

State Local Cybersecurity Grant Updates Program

WaTech
Washington Technology Solutions

SLCGP review

- From the Infrastructure Investment Jobs Act - $1B
- 4-year program – WA has approximately $3M / year one
- Planning Committee stood up; WA Plan written; 16 required elements addressed; Plan complete
- Application nearing completion
- Notice of Intent – 100+ interested local governments at $15M+ in proposals
- First year project selection by end of July

Current WA SLCGP Timeline

- 6/2: Notice of Intent closed
- 6/6: Planning Committee Meeting – Plan adopted
- Mid June – Mid July: Application period – 4 weeks
- 6/30: Plan submitted to CISA for approval (completed week of June 12)
- 7/10-14: Initial application review
- 7/17-21: Selection process
- 7/24-26: Notify successful applicants
- 7/24-8/2: Package projects; revise Investment Justification; resubmit to FEMA
- mid-Sept – end of Oct: Agreements completed; funding released

WA Cybersecurity Plan

- Plan reflects a lot of work across two agencies and should be a great guide for local governments to not only apply for SLCGP grant funding, but also move towards a stronger cybersecurity posture.
- Writing group – consisting of subject matter experts from both WaTech and MIL-EMD.
- Adopted by Planning Committee 6/6/23

- Information here:

https://watech.wa.gov/State-Local-Cybersecurity-Grant-Program

Communications, Important links, Resources, Application, Criteria

WaTech
Washington Technology Solutions

Legislative Session Updates

WaTech
Washington Technology Solutions

SSB 5518 – Creation of the Cybersecurity Advisory Committee as a Subcommittee of the Emergency Management Council

Purpose: **Provide advice and recommendations that strengthen cybersecurity** in both industry and public sectors **across all critical infrastructure sectors**.

Membership: Organizations with expertise and responsibility for cybersecurity and incident response - local government, tribes, state agencies, institutions of higher education, the technology sector, and first responders.

Activities:

- **Identify which local, tribal, and industry infrastructure sectors are at the greatest risk of cyberattacks** and need the most enhanced cybersecurity measures.
- Use federal guidance to **analyze categories of critical infrastructure in the state** that could reasonably result in catastrophic consequences if unauthorized cyber access to the infrastructure occurred.
- **Recommend cyber incident response exercises** that relate to risk and risk mitigation in the water, transportation, communications, health care, elections, agriculture, energy, and higher education sectors.

- Meet quarterly, and at least once a year, hold a joint meeting with the cybersecurity advisory committee created with the Military Department.
- By December 1, 2023, and each December 1 after, **provide a joint report produced by the Military Department and WaTech specifying recommendations considered necessary to address cybersecurity in the state.** The TSB security subcommittee is responsible for coordinating any recommendations made in the report.

WaTech
Washington Technology Solutions

SSB 5518 – Creation of the Technology Services Board Security Subcommittee

Purpose: Provide advice, recommendations, and policy that strengthen cybersecurity in the state.

Membership: Comprised of a subset of members appointed to the board, as determined by the chair of the technology services board. **The chair may make additional appointments to the technology services board security subcommittee** to ensure that relevant technology sectors are represented.

Activities:

- **Review emergent cyberattacks and threats** to critical infrastructure sectors in order to identify existing gaps in state agency cybersecurity policies.
- **Recommend tabletop cybersecurity exercises**, including data breach simulation exercises.
- **Review the proposed policies and standards** developed by the office of cybersecurity.
- **Review information relating to cybersecurity incidents and ransomware incidents** to determine commonalities and develop best practice recommendations for public agencies.
- Meet quarterly, and at least once a year, hold a joint meeting with the cybersecurity advisory committee created with the Military Department.
- By December 1, 2023, and each December 1 after, **provide a joint report produced by the Military Department and WaTech specifying recommendations considered necessary to address cybersecurity in the state.**

WaTech
Washington Technology Solutions

SCIP Goals Workshop

Vision:

Seamless interoperable and resilient communications

Mission:

Enable a statewide interoperable public safety communications strategy

SIEC SCIP Principles

- SCIP is the strategic plan for the SIEC
- Regularly review and update the SCIP
- Action plan for all objectives
- Measurable results and communication of progress
-
- Member and committee ownership
- Regular report outs

Washington's implementation plan is shown in the table below.

Goals	Objectives	Owners	Completion Date
1. **Enhance and expand Interoperable Communications governance throughout the state**	1.1 Research and implement opportunities for regional and/or discipline representation (e.g., SIEC work groups including regional working groups)	SIEC	December 2023
	1.2 Develop and execute a communications plan to provide information and encourage active participation across the state		September 2023
	1.3 Identify and establish subcommittees and subcommittee structure to add to the SIEC (ex. cybersecurity)		June 2023
	1.4 Identify grant opportunities and communicate opportunities to stakeholders		Ongoing
	1.5 Create a full-time, fully-funded SWIC position through identification of roles and responsibilities, sustainable funding stream, and administration staff support		July 2023
	1.6 Formalize communication and coordination between the state broadband office and the SIEC		March 2023
	1.7 Identify the SIEC's role in alerts and warnings across the state		June 2023

Click to edit Master title style

1. Continue to improve the cybersecurity posture of interoperable systems	4.1 Increase information sharing between the Office of Cybersecurity and the SIEC	State CISO	Ongoing
	4.2 Provide templates and communicate best practices for cybersecurity	CISO	Ongoing
	4.3 Add the state CISO to the SIEC	SIEC	February 2023

SCIP Update Workshop

- Utilize the next SIEC meeting.
- Hybrid workshop.
- Update the SCIP Objectives, Owner, and Completion Dates.
- Create action plans for each near-term objective (next 3 to 6 months).

Public Comment