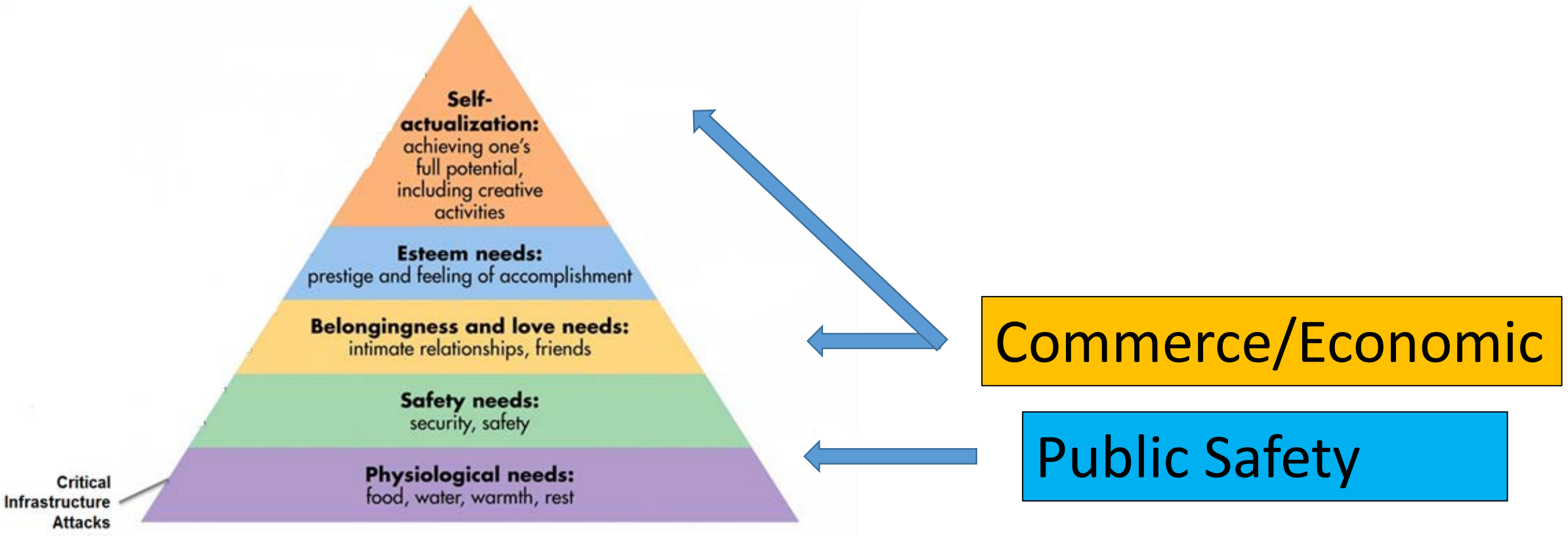
# Federal & Domestic Cyber Operations Capabilities

# Understanding Critical Infrastructure Security/Resilience

**16 Sectors**
**85% in the Private Sector**

# Securing Critical Infrastructure – A “Maslow-like” approach

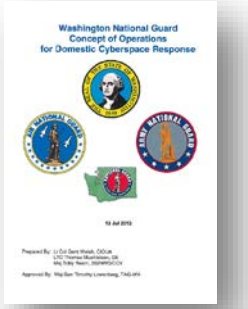
Cyber threats have already challenged public trust and confidence in global institutions, governance, and norms, while imposing costs on the global economy. These threats pose an increasing risk to public safety, as cyber technologies are integrated with critical infrastructure in key sectors. The breadth of cyber threats posed to U.S. national and economic security has become increasingly diverse, sophisticated, and serious, leading to physical, security, economic, and psychological consequences. – *James R. Clapper, Director of National Intelligence, 5 January 2017*

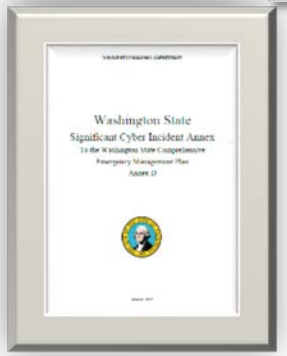


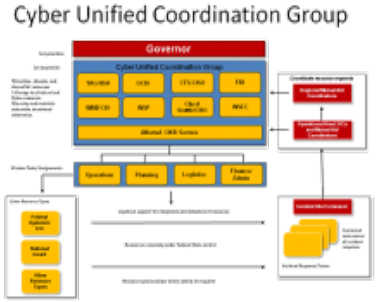

Source: OPTIV.com

# WASHINGTON MILITARY DEPARTMENT

# Securing Washington's Cyber Critical Infrastructure



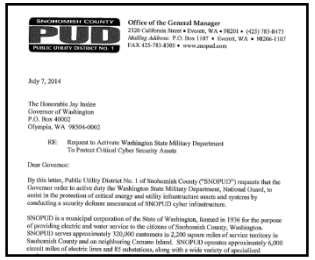


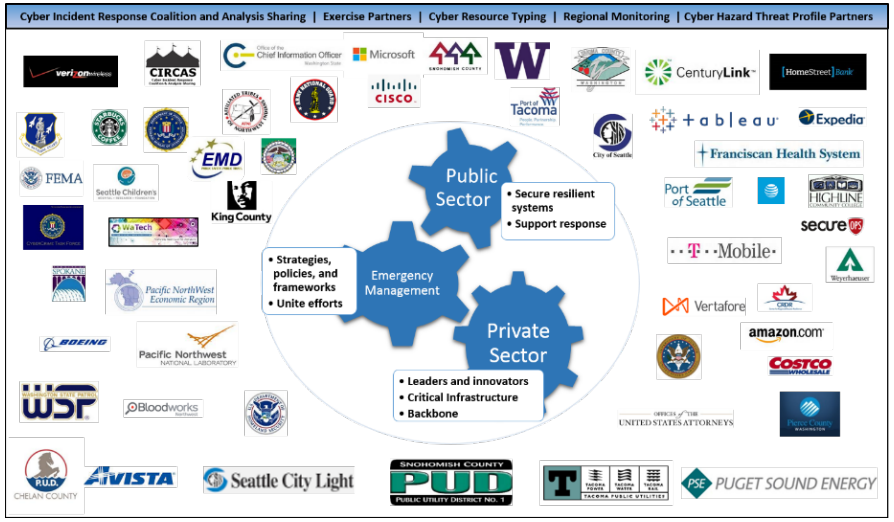




Policy/Authorities

Capabilities

Outreach



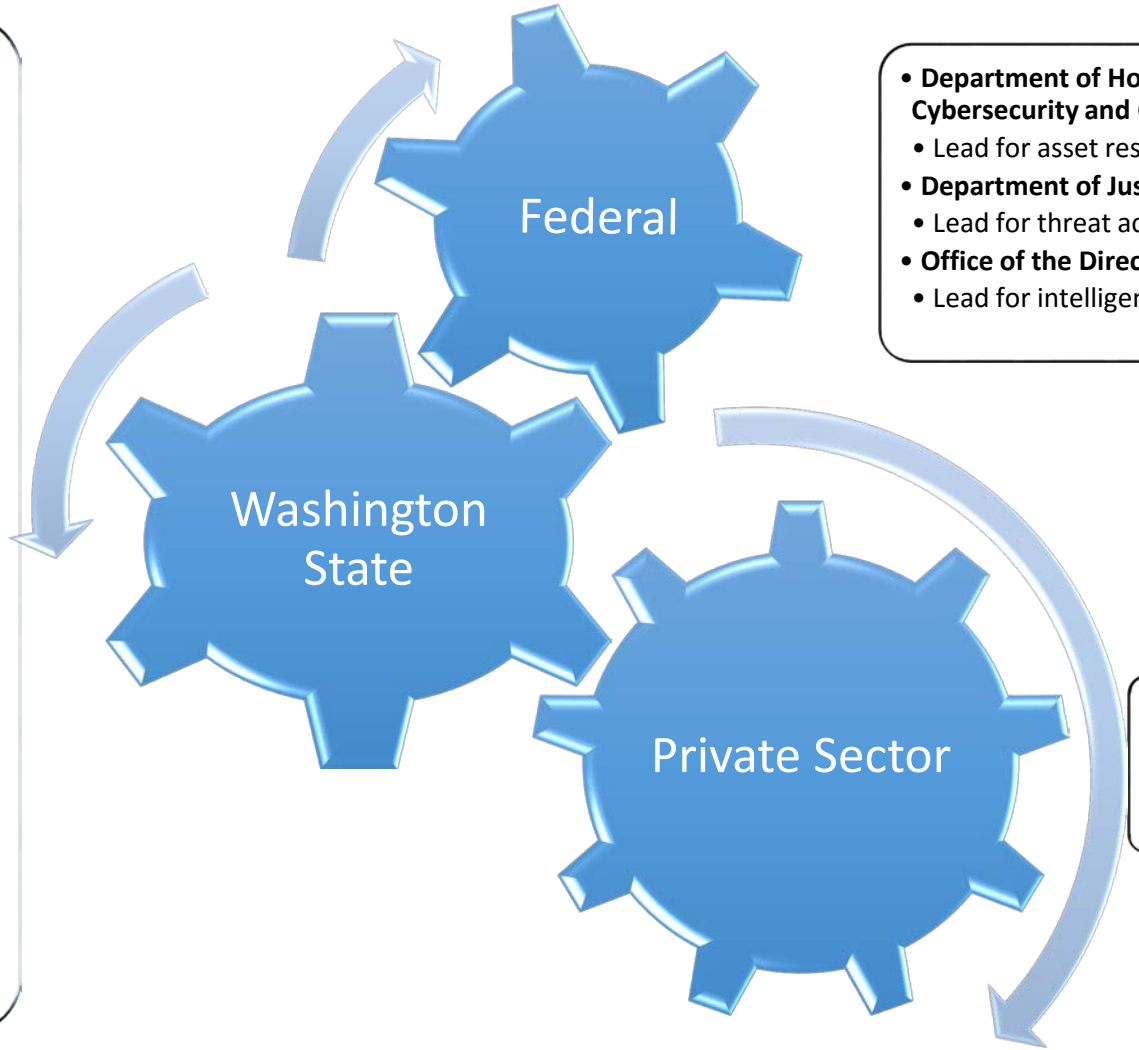




**Emergency Management Council/ Infrastructure Resilience Subcommittee**

- All 16 sectors represented
- 92 members (47 private/45 government)

# Securing Critical Infrastructure: Roles and Responsibilies

- **Washington Military Department**
  - RCW 38-52
  - Natural, technological, or human caused events
  - State Homeland Security Advisor
  - Designated Senior Official for significant cyber security incident
  - National Guard/State Guard
  - EMD (Cybersecurity Manager, Critical Infrastructure, Private/Public Partnerships)
- **OCIO/OCS/WaTech**
  - State CIO
  - State technology issues
  - State Government networks
  - Cybersecurity for state government
- **Utilities and Transportation Commission**
  - Ensures private utilities and carriers implement cybersecurity measures
- **Department of Commerce**
  - Promotes state as prime location for IT and cybersecurity




- **Department of Homeland Security/National Cybersecurity and Communications Integration Center**
  - Lead for asset response
- **Department of Justice (FBI)**
  - Lead for threat activities
- **Office of the Director of National Intelligence**
  - Lead for intelligence support

- **Leaders and innovators**
- **Critical Infrastructure owners/operators**
- **Backbone**

# National Guard Cyber Evolution

1998 — 2000 — 2005 — 2010 — 2011 — 2014 — 2016

**Information Warfare Team (1998-2000)**

"A Twinkle in a General's Eye…"
Environment: ANG Reset, BRAC, Mission Sunsets
Defining the ANG IW Model, Recruiting and building the skills base

**262d Information Warfare Aggressor Squadron (2000-2005)**

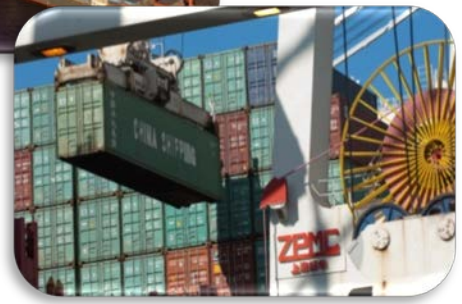
Concept of Operations: NIA, CIIVA
USAF & Congressional Investments to build CIP Capabilities
Common TTPs (NSA, DISA, AFWIC/AFIOC)

**262d Information Warfare Aggressor Squadron (2005-2010)**

Developed ICS assessment methodologies and training
Formalized Hunt/ICS training IAW AFSPC requirement
Enhanced Cyber Support to WA State & DoD

**262d Network Warfare Squadron (2010-2014)**

2014 CMF PAD-ICS CPT, Project C
AFCEC/248th partnership
35 CVA certified Operators and 8 SEE's



**143d Information Operations Squadron (2011-2014)**

Transition from Combat Communications to Cyber Hunt capability
Created "DCO-101", now delivered as I-PQT for all AF Cyber Operators
35 CVA certified Operators and 8 SEE's

**256th Intelligence Squadron(2011-2014)**

Transition from Combat Communications to Digital Network Intelligence
Worked with NSA out of Yakima

**2016 and beyond**

Cyberspace Operation Group / Cyberspace Operations Sq
IOC/FOC to meet CPT deployment

# National Guard Cyber Capabilities

Cyber Ops Support

Security Remediation

Cyber Mission Planning

Situational Awareness

Vulnerability Assessment

**262d NWS & 143rd IOS first ANG CPT's mobilized for COCOM**

# Domestic Operations

Presenting Federal capabilities to the Governor

- Basic Network Vulnerability Assessments
- Industrial Control Systems Defensive Assessments

Can also employ under CPT methodology

- Evaluate by mission rather than system
- Integrate with community cyber approach

C2 performed under a joint construct

- WARNORD and OPORD
- Understanding authorities critical to success
- Customer owns their own data

# ICS Employment

- **POTUS directed - Minuteman III vulnerability assessment to identify opportunities to strengthen the security posture of the national command and control capability**

***CBS News, 60 Minutes, Who's minding the nukes – July 13, 2014***

WASHINGTON AIR NATIONAL GUARD

# Snohomish County Public Utility District Cyber Assessment

# Steps to Success

## Governor appointed TAG

STATE OF WASHINGTON
OFFICE OF THE GOVERNOR

April 1, 2013

Major General Bret D. Daugherty
The Adjutant General
Washington Military Department
Building 1, MS: TA-20
Camp Murray, WA 98430-5000

RE: Designation as Senior Official and Primary Agency for Cyber Security Coordination

Dear General Daugherty:

In accordance with Appendix H of the National Cyber Incident Response Plan and your status as the Adjutant General and Homeland Security Advisor for the state of Washington, I am appointing you as the Senior Official to represent the state of Washington for management and coordination of cyber security issues both within the state and at the federal level.

Additionally, to provide unity of effort and a "whole government" approach in all phases of cyber incident planning across all levels of state government, I am directing state agency heads to ensure that all communications and coordination regarding cyber security matters be directed to the Military Department. The Military Department, through the Cyber Integrated Project Team, will ensure a coordinated statewide planning perspective in all matters of cyber security.

The Military Department is also hereby designated as the Primary Agency for external communication with the Department of Homeland Security for all cyber security matters within state government to include future training, exercises and planning coordination, as well as the Lead Agency that provides the official position of the state on cyber matters to our federal partners.

The threat of a catastrophic cyber event occurring within the state of Washington is increasing daily and effective planning and coordination activities that support unity of effort across the whole of state government is essential to successfully meeting this challenge.

Very truly yours,

Jay Inslee
Governor

"I am appointing you as the Senior Official to represent the state of Washington for management and coordination of cyber security issues both within the state and at the federal level."

## Authorized Activation Authority to TAG

STATE OF WASHINGTON
OFFICE OF THE GOVERNOR

April 1, 2013

Major General Bret D. Daugherty
The Adjutant General
Washington Military Department
Building 1, MS: TA-20
Camp Murray, WA 98430-5000

RE: Activation of Members of the Washington State Guard and National Guard to Conduct a Security Defense Assessment of Selected State Agencies

Dear General Daugherty:

Over the last 10 years, the people of this state have led the way in developing and adopting a vast array of information technology cyber infrastructure. Our citizens, businesses and government have integrated this cyber infrastructure into nearly every aspect of daily life, driving everything from simple communications, travel and daily business operations, to scientific innovations and international trade.

However, our cyber infrastructure is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and data available through our cyber infrastructure can be compiled for nefarious purposes. Because of our dependence on and the risks in our cyber infrastructure, it is critical that assessments be performed to secure the cyber infrastructure of Washington State. The potential threats to our information technology infrastructure and the private information contained on those systems create a threat to the citizens and economy of our state.

The Washington State Military Department possesses a number of unique and valuable cyber infrastructure assessment capabilities, with certain State Guard and National Guard members possessing highly specialized training in security defense assessments of cyber infrastructure. The Military Department has agreed to use these specialized resources to conduct security defense assessments of selected state agencies. To accomplish this work, it will be necessary to activate a small number of members of the organized militia in a temporary State Active Duty status.

The Military Department may enter into agreements with selected state agencies to conduct security assessments of our cyber infrastructure. Any members of the organized militia placed into active state service must be paid from funds already appropriated to the Military Department, or with funds reimbursed to the Military Department from other state agencies or federal grants.

Major General Bret D. Daugherty
April 1, 2013
Page 2

Protection of our state and nation's cyber infrastructure is essential to securing sensitive, personal and private information from exploitation through computer network vulnerabilities, including criminal terrorist acts that significantly disrupt the economy and the conduct of government. Performance of this work by the Military Department is required to identify, prepare for and protect against system vulnerabilities in our cyber infrastructure that could compromise the safety or welfare of our citizens.

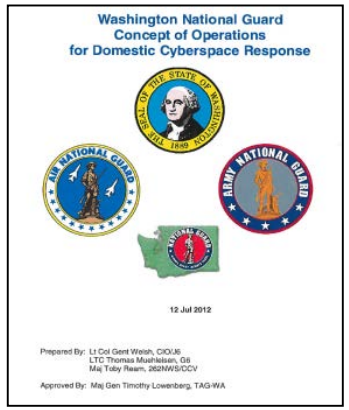
Therefore, I, Jay Inslee, Governor of the state of Washington, acting pursuant to RCW 38.08.040, order into active state service members of the organized militia of Washington State, to include the National Guard and State Guard, as may be necessary in the opinion of the Adjutant General of the Washington State Military Department, to perform such duties as the Adjutant General deems appropriate for the circumstances described above. This order shall be effective immediately and until revoked.

Very truly yours,

Jay Inslee
Governor

"order into active state service members of the organized militia of Washington State,

to include the National Guard and State Guard, as may be necessary"

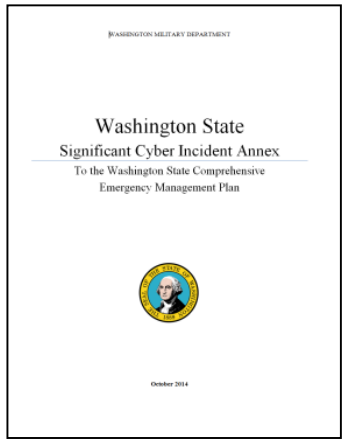

Washington National Guard
Concept of Operations
for Domestic Cyberspace Response

12 Jul 2012

Prepared By: Lt Col Gent Welsh, CIO/J6
LTC Thomas Mushlesen, G6
Maj Toby Ream, 262NWS/OCV

Approved By: Maj Gen Timothy Lowenberg, TAG-WA

We built a CONOP for how to proceed


WASHINGTON MILITARY DEPARTMENT

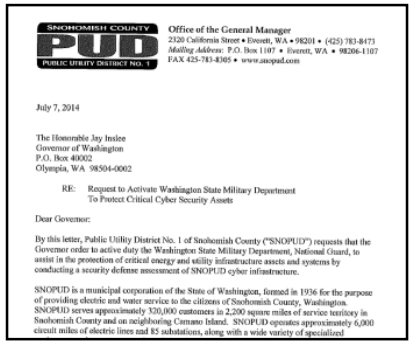
Washington State
Significant Cyber Incident Annex
To the Washington State Comprehensive
Emergency Management Plan

October 2014

And developed a Cyber Annex to the state Emergency Management Plan

# Mission Authority

## GM Request to Governor



SNOHOMISH COUNTY PUD
PUBLIC UTILITY DISTRICT NO. 1

Office of the General Manager
2320 California Street • Everett, WA • 98201 • (425) 783-8473
*Mailing Address:* P.O. Box 1107 • Everett, WA • 98206-1107
FAX 425-783-8305 • www.snopud.com

July 7, 2014

The Honorable Jay Inslee
Governor of Washington
P.O. Box 40002
Olympia, WA 98504-0002

RE: Request to Activate Washington State Military Department To Protect Critical Cyber Security Assets

Dear Governor:

By this letter, Public Utility District No. 1 of Snohomish County ("SNOPUD") requests that the Governor order to active duty the Washington State Military Department, National Guard, to assist in the protection of critical energy and utility infrastructure assets and systems by conducting a security defense assessment of SNOPUD cyber infrastructure.

SNOPUD is a municipal corporation of the State of Washington, formed in 1936 for the purpose of providing electric and water service to the citizens of Snohomish County, Washington. SNOPUD serves approximately 320,000 customers in 2,200 square miles of service territory in Snohomish County and on neighboring Camano Island. SNOPUD operates approximately 6,000 circuit miles of electric lines and 85 substations, along with a wide variety of specialized

## Governor Go-Do to TAG

JAY INSLEE
Governor

STATE OF WASHINGTON
Office of the Governor

December 22, 2014

Major General Bret Daugherty
The Adjutant General
Washington Military Department
Building 1, MS: TA-20
Camp Murray, WA 98430-5000

RE: Activation of Seven Members of the Washington State Guard and National Guard to Conduct a Cyber Security Defense Assessment for the Snohomish County Public Utility District No. 1

Dear General Daugherty:

Over the last 30 years, the people of this state have led the way in cyber innovation and the utilization of vast arrays of information technology systems and infrastructures. Our citizens, businesses and government have integrated cyber capabilities into nearly every aspect of daily life, driving everything from communications, medical care and business operations to education, scientific innovation, industrial production and international trade.

Unfortunately, these indispensable cyber systems and infrastructures are also vulnerable to a wide variety of threats that expose the citizens, government and economy of Washington State to exploitation and harm. Regardless of their origin, whether intentional or accidental, manmade or natural, it is essential that appropriate security defense assessments and testing be performed to identify, prepare for and protect against vulnerabilities to governmental systems and infrastructures that threaten the health, safety and welfare of our citizens.

The Snohomish Public Utility District #1 (SNOPUD) relies upon critical information technology systems and infrastructures in performing its public duties, the protection of which is essential to securing sensitive, personal and private information from exploitation through computer network vulnerabilities. Performance of security defense assessments and testing to protect these information technology systems and infrastructures is required to identify, prepare for and protect against system vulnerabilities that will compromise the security of this information.

The Washington State Military Department possesses valuable cyber systems and infrastructure security assessment and testing capabilities due to the mix of citizen soldiers and airmen in its cyber defense units. These highly skilled members draw expertise from formal military training

Major General Bret Daugherty
December 22, 2014
Page 2

and civilian experience. The Military Department has agreed to use these specialized resources to conduct security defense assessments and testing identified by SNOPUD as critical to the protection of its governmental operations, and the health, safety and welfare of our citizens.

To accomplish this work, it will be necessary to place seven members of the Washington National Guard and State Guard in a temporary State Active Duty status.

Any costs or expenses associated with this work must be paid from funds appropriated to the Military Department or with funds reimbursed to the Military Department from the Office of the Chief Information Officer pursuant to an interagency agreement. The costs associated with this activation shall not exceed $15,000.

Therefore, I, Jay Inslee, Governor of the state of Washington, acting pursuant to RCW 38.08.040, order into active state service seven members of the Washington National Guard and State Guard, as may be necessary in the opinion of the Adjutant General of the Washington State Military Department, to perform such duties as the Adjutant General deems appropriate for the circumstances described above.

Very truly yours,

Jay Inslee
Governor

Memorandum of Agreement Between
the Washington State Military Department
and
the Snohomish County Public Utility District No. 1

I. PARTIES

The parties to this Memorandum of Agreement (MOA) are the Washington State Military Department (MIL), and the Snohomish County Public Utility District No. 1 (SNOPUD) (collectively, "the agencies"). MIL is authorized to enter into this MOA under RCW 39.34 and SNOPUD is authorized under RCW 54.16.085 and RCW 39.34.

II. PURPOSE

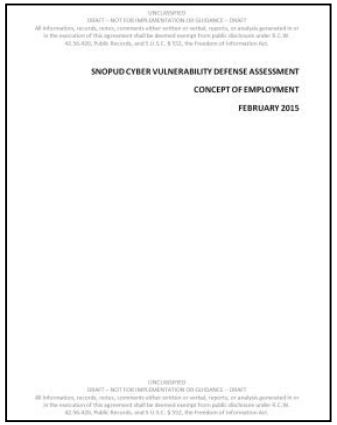
The agencies signing below know the risks of network attack and appreciate the need to secure sensitive information and personal-private information from exploitation through computer network vulnerabilities, including criminal terrorist acts that significantly disrupt critical infrastructure [1] and is consistent with Presidential Policy Directive 21, Critical Infrastructure Security and Resiliency, and Executive Order 13636, Improving Critical Infrastructure Cybersecurity. SNOPUD requested Washington State Governor Jay Inslee, pursuant to RCW 38.08.040, to order into active state service specialized unit members of the Washington State and National Guard to conduct cyber security defense assessments and testing of SNOPUD critical energy and utility assets and systems for protection of the public health, welfare and safety. In granting this request, Governor Inslee ordered The Adjutant General of the MIL to direct performance of such duties by appropriate members of the Washington State and National Guard pursuant to agreement with SNOPUD identifying the assessments and testing critical to public health, welfare and safety, and addressing reimbursement of costs to MIL. The vulnerability assessments and testing will aid SNOPUD in understanding the assessment process, determining risk, and establishing a baseline for future assessments; these activities are critical to securing cyber critical infrastructure of SNOPUD and the public health, welfare and safety of the citizens, economy and public interests of Washington State.

Under this MOA, MIL will conduct a security defense assessment of SNOPUD cyber critical infrastructure. Specifically, SNOPUD requests that a Defense Assessment Team from the MIL test and evaluate SNOPUD computer networks, IT Staff, and users in order to determine and address issues affecting SNOPUD cyber critical infrastructure. The Assessment Team shall be placed on State Active Duty status for this purpose.

III. BACKGROUND

[1] As defined in the Critical Infrastructure Protection Act of 2001, "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (42 U.S.C. 5195c(e)).

JAG's helped to build an MOA



UNCLASSIFIED
DRAFT – NOT FOR IMPLEMENTATION OR GUIDANCE – DRAFT
All information, records, notes, comments either written or verbal, reports, or analysis generated in or in the execution of this agreement shall be deemed exempt from public disclosure under R.C.W. 42.56.420, Public Records, and 5 U.S.C. § 552, the Freedom of Information Act.

SNOPUD CYBER VULNERABILITY DEFENSE ASSESSMENT

CONCEPT OF EMPLOYMENT

FEBRUARY 2015

UNCLASSIFIED
DRAFT – NOT FOR IMPLEMENTATION OR GUIDANCE – DRAFT
All information, records, notes, comments either written or verbal, reports, or analysis generated in or in the execution of this agreement shall be deemed exempt from public disclosure under R.C.W. 42.56.420, Public Records, and 5 U.S.C. § 552, the Freedom of Information Act.

We built CONEMP as a mission plan

# Assessment of a Public Utility

- Scope and developed initial COA
  - Assessment of a Municipal Corporation
  - Operators on State Active Duty (not T-32, not T-10)
  - OPCON passed to the State Joint Operations Center
  - Warning order was issued and Initial team selection began
    - Begin sourcing equipment/resources and planning
    - Traditional assessment methodology with some tweaks
      - ROE
      - Preapproved Actions
      - Trusted Agent model

# Assessment of a Public Utility

- Team Composition (Operations)
  - (1) Maj – Mission Commander
  - (2) Maj, (1) Captain, (1) LT, (1) MSgt, (1) SSgt
  - Microsoft, T-Mobile, Security Startup, Bank
  - Joint Team brought together for the first time WA ANG, WA ARNG, WA State Guard

- Command and Control
  - Mission over a two week time period
  - Pure remote operation
  - Daily updates to trusted agent and state JOC
  - “Don’t Cross the Streams” (Title 32/10 and SAD)
  - Introduction of a “Hunter” component into mission

# Assessment of a Public Utility

- Access Recon - indicated a need for tailored access
  - Started with Standardized Preapproved Actions and Tactics
    - Assessment team developed full package for access and escalation
    - Persistent access to the target organization
    - Custom mechanisms to defeat corporate security infrastructure
    - Complete privileged control of the network
    - Access to Power Generation and Distribution
    - Access to Water Systems

**From:** iPad Survey [mailto:surveys@[redacted]

**Sent:** Tuesday, February 24, 2015 11:03 AM

**To:** iPad Survey

**Subject:** Mobile Workforce Survey

The [redacted] PUD has begun exploring the benefits of issuing iPad tablet technologies to employees in various roles. The roles being considered at this time include engineering, operational and administrative roles. A limited number of employees will be asked to complete a mobile workforce survey. A number of those employees who complete the survey will be selected to pilot our initial round of tablet technologies. This program is only available to CURRENT, ACTIVE FULL TIME [redacted] employees (retirees and contractors are NOT eligible). If you'd like to participate in the program, please complete the following survey. The initial phase is limited to a small number of employees, please do not share the survey link or discuss the program with other employees.

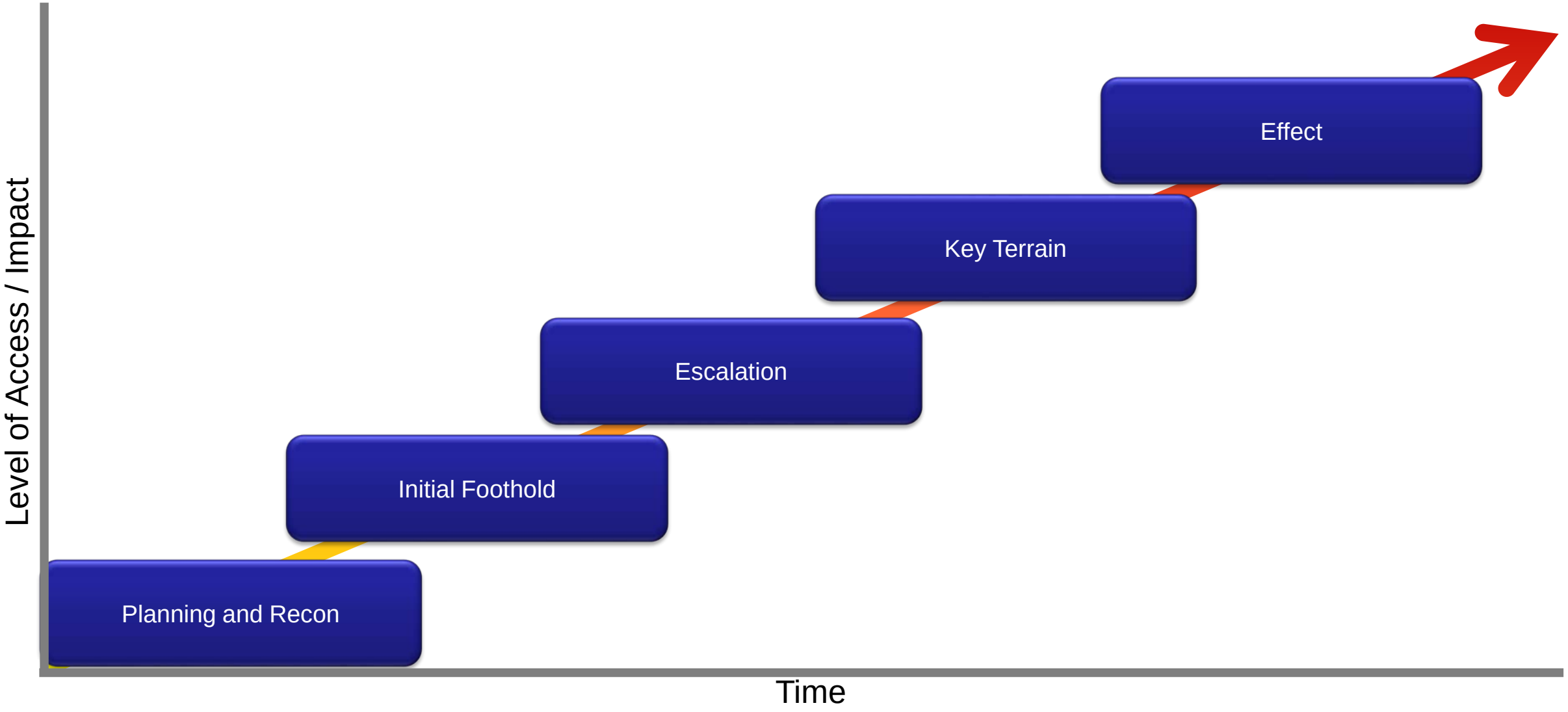
http://MobileWorkforceSurvey.[redacted].com/ActiveEmployeesOnly.asp

If you have any questions, please contact surveys@[redacted]. We're looking forward to seeing your response!

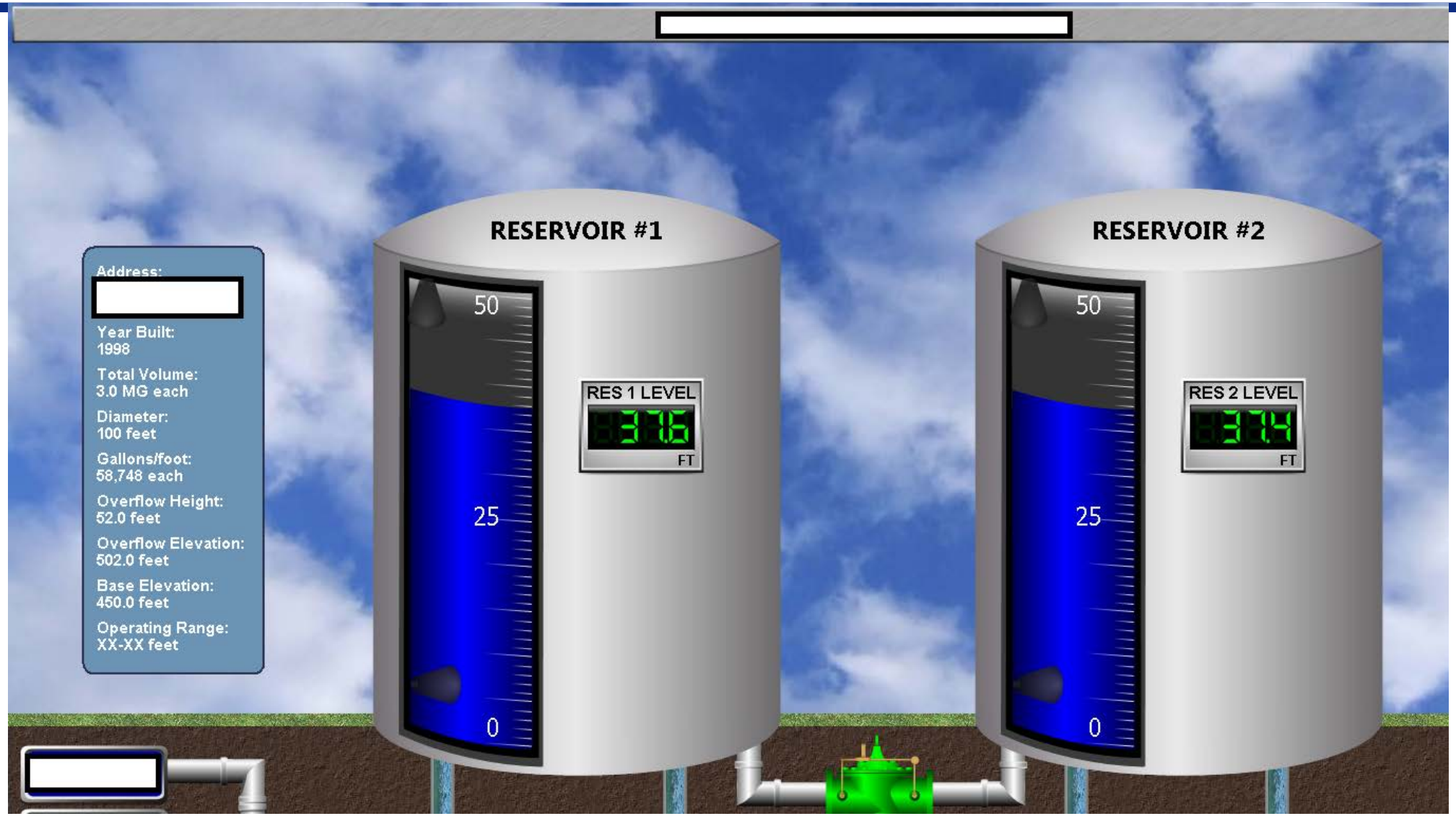
Respectfully,

The Mobile Workforce Team

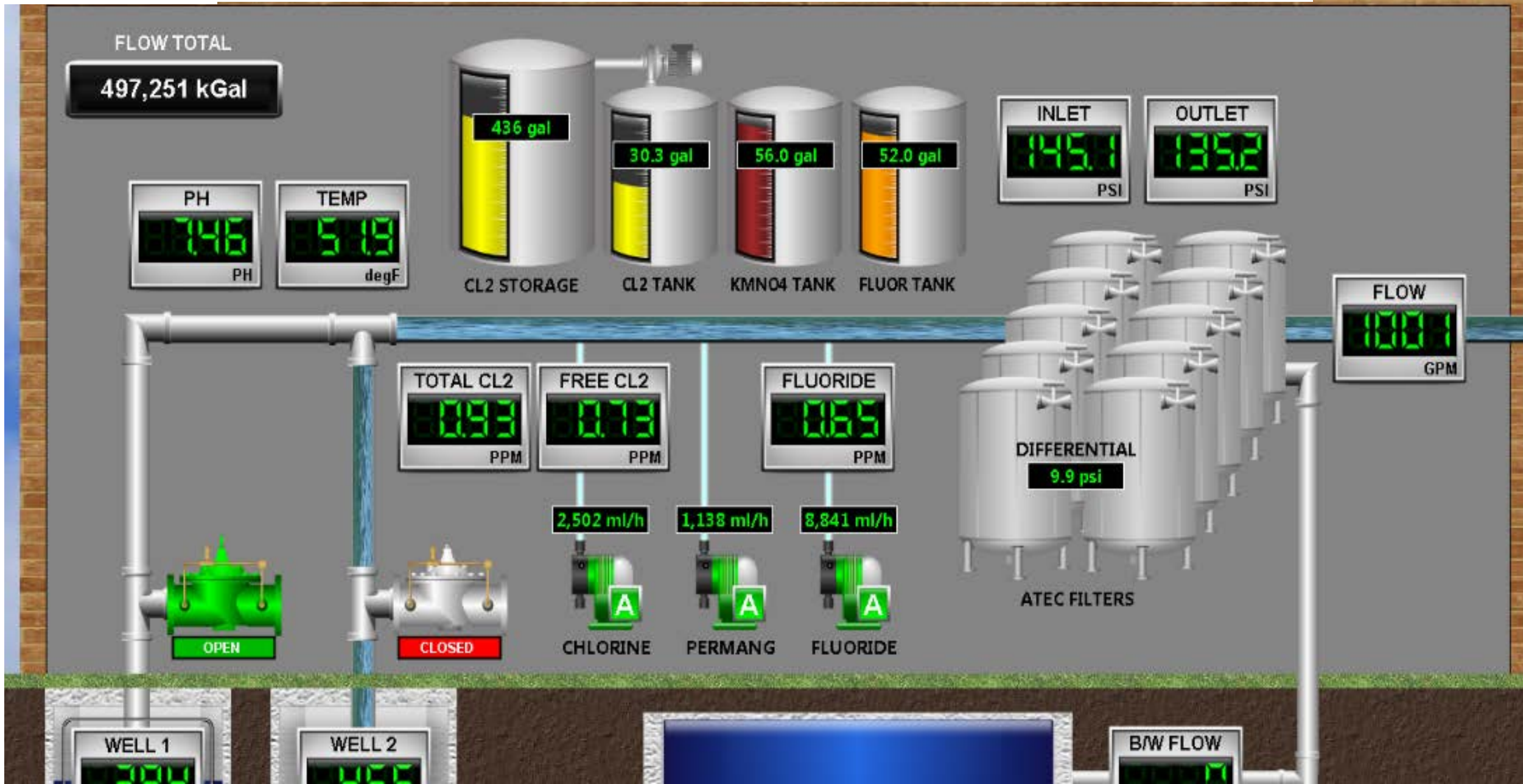
# Attack Flow


Level of Access / Impact
Planning and Recon
Initial Foothold
Escalation
Key Terrain
Effect
Time

# Water Reservoir Controls

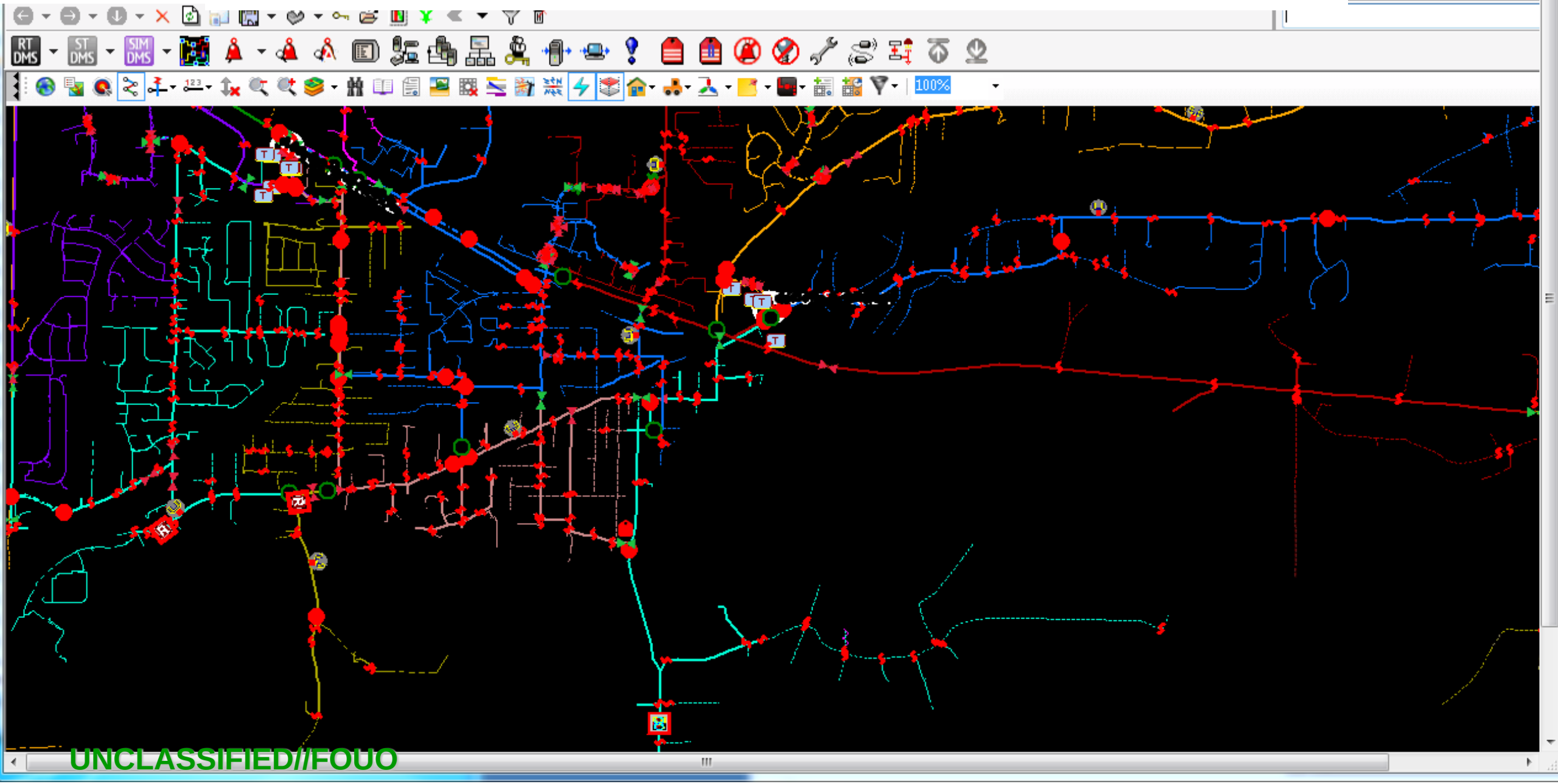


# Water mixture Controls



WASHINGTON AIR NATIONAL GUARD

# Power Grid Controls




UNCLASSIFIED//FOUO

# Assessment of a Public Utility

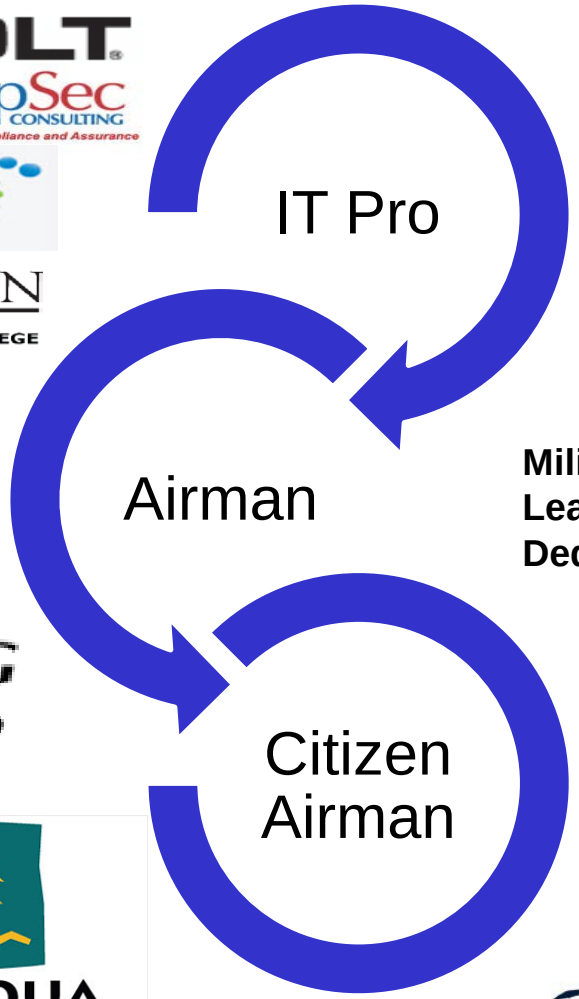
Demonstrated the capability to **disrupt power and water services** to a significant portion of WA state

# Strategic Implications

- Instrument of National Power
  - Cyber security talent available to State Governors and ANG
  - Operations under the correct title authorities enables action without Stafford Act
  - Tailored and focused assessment and assistance services - strengthened Defensive posture of Public Utility

- Resource Considerations
  - Assessment cost < $20,000
  - Comparable assessment from the private sector > $150,000
  - State Leadership is pushing for a focus on Critical Infrastructure

# The Citizen Airman/Soldier




- Business Acumen
- Industry Leadership
- Technical Experience

Military Training/Expertise
Leadership
Dedication, Esprit de Corps

- Well-rounded/Dynamic
- Technically Savvy
- Depth of Capability