

Office of Special Investigations



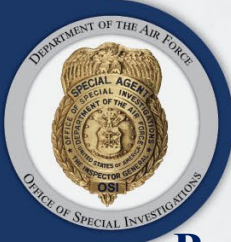
Threats to the Sentinel Intercontinental Ballistic Missile (ICBM) System



Shelby Skopik
OSI/8FIR CI Branch

06 AUG 2025

Sentinel Background

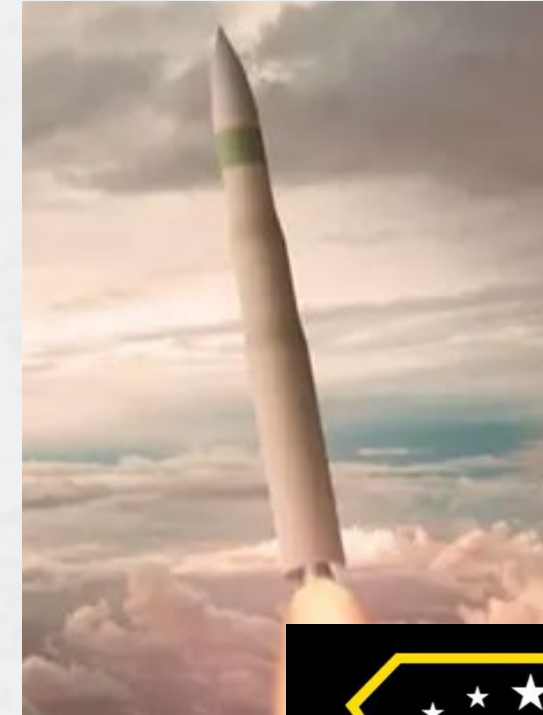


Program Origin

- **9 SEP 2020:** USAF awards USPER Northrop Grumman \$13.3 billion to modernize the U.S. Minuteman III (MMIII) ICBM system to the Sentinel program
- **Early 2024:** MMIII replacement trips critical cost breach, requiring program review by U.S. congress, and causing delays to Sentinel IOC by at least 2 years (estimated mid-2029/2030)

Function and Timeline of Sentinel Sites

- Vandenberg SFB, CA – Testing Site - First Flight (Estimated 2027/2028)
- Hill AFB, UT – Maintenance Site (Estimated 2026– Program Decommissioning)
- F.E. Warren AFB, WY – Possible First Site for MMIII to Sentinel Conversion (Dates to be confirmed)
- Malmstrom AFB, MT – Possible First Site for MMIII to Sentinel Conversion (Dates to be confirmed)
- Minot AFB, ND - Third Site for MMIII to Sentinel Conversion (Dates to be confirmed)



Sentinel at F.E. Warren AFB

Estimated Construction Timeframe: 2025 - 2038

Construction Activities:

- All 150 Launch Facilities (LFs) and 15 Missile Alert Facilities (MAFs) will be renovated and modernized
 - Program goal is to renovate one LF per week and ~12 months to renovate each MAF
- Establishment of new utility corridors
 - ~900 miles of underground utility corridors and 16 foot wide property easements would be established from FEWAFB to and throughout the missile fields
- Temporary establishment of workforce housing camp
 - Housing for up to 3,000 construction and security workers and support personnel for 2-5 years
- All MMIII-related components from LFs and MAFs brought to FEWAFB for sorting, demilitarization, and disposal
 - Existing MMIII maintenance and security operations will continue through conversion



(U) Excavator Digging Large Trench For Utility Installation



(U) Construction at MMIII Launch Facility



Sentinel Project for F.E. Warren AFB



OFFICE OF SPECIAL INVESTIGATIONS

Size of Sentinel Project for FEWAFB

- FEWAFB occupies 5,866 acres west of Cheyenne in Laramie County
- The FEWAFB Missile Field spans an area the size of Vermont
- The FEWAFB Missile Field covers approximately 9,600 square miles throughout seven counties and three states
 - Wyoming: Goshen and Laramie counties
 - Nebraska: Banner, Kimball, and Cheyenne counties
 - Colorado: Weld and Logan counties

Physical Vulnerabilities and Considerations

- A railway transits through FEWAFB
- Hills surrounding FEWAFB allow some visibility for on-base activities
- The FEWAFB Missile Field facilities are surrounded by private land and are often in rural locations
 - Though heavily guarded, local LE and community members may observe suspicious behavior before USAF Security Forces



(U) Minuteman III Launch Facility



(U) Train Going Through FEWAFB

Historic Foreign Intelligence Interest in Missiles

American Spies Who Have Provided Missile Data to Adversaries:

- Benjamin Bishop (China)
- Noshir Gowadia (China, Israel, Germany, and Switzerland)
- Ariel Weinmann (Russia)
- Subu Kota (USSR)
- Ben-Ami Kadish (Israel)
- Stewart Nozette (Israel; Attempted)
- Robert Hoffman (Japan)
- Stephen Jin-Woo Kim (Media Leak)



Why Are Foreign Intelligence Entities Interested in Sentinel?



Russia:

- Russia continues to develop long-range nuclear-capable missiles meant to penetrate or bypass U.S. missile defenses

China:

- China is building hundreds of new ICBM silos and modernizing their intercontinental strike capability
 - Interested in U.S. missile technology for technology transfer and intellectual property theft
 - Interested in Chinese ICBM survivability and countermeasures

Iran:

- Iran's ballistic missile programs pose a threat to U.S. assets and allies in the Middle East
- Want to maintain awareness of U.S. missile capabilities that may hinder the effectiveness of Iran's missile strike capabilities in the Middle East

North Korea:

- Kim continues to prioritize efforts to build a capable missile force designed to evade U.S. missile defenses

Foreign Intelligence Threat to Sentinel

Russia, China, and Iran are almost certainly interested in collecting technological and operational information regarding Sentinel. U.S. strategic deterrent systems have historically been a high-priority target for America's adversaries.

Foreign Intelligence Collection Techniques:

- **Open-Source Information:** Russia, China, and Iran likely rely on open-source information on Sentinel to fulfill intelligence collection requirements and focus future intelligence collection efforts.
- **Cyber Operations:** Russia, China, and Iran have been known to conduct offensive cyber operations in order to obtain sensitive but unclassified information on U.S. military weapons systems, and to conduct influence operations.
- **Human Intelligence:** Russia, China, and Iran have been known to use the following methods to conduct human intelligence on U.S. military weapons systems.
 - Elicitation at conferences and events
 - Foreign students and academic exchanges
 - Social media and professional networking sites
 - Foreign companies and business exchanges
 - Unsolicited requests (email, phone, or social media) targeting U.S. cleared defense contractors
 - And of course, honeypots...



Foreign Intelligence Case Study



USPER Benjamin Pierce BISHOP

- Retired U.S. Army Lt Col working at U.S. Pacific Command
- Met a 27 year old Chinese graduate student, became friends then lovers
- Chinese student asked for advice and sources for her graduate research
- BISHOP began bringing her classified documents to review
- BISHOP also emailed SECRET-level documents on:
 - Missile defense systems
 - Early warning radar systems
 - Nuclear war plans and strategies
- Was arrested in 2013, plead guilty, and was sentenced to 7+ years in prison



Key Takeaway: The BISHOP case study shows that China is willing and able to conduct human intelligence operations to obtain information on U.S. missile systems.

Local Area Threats to Sentinel



General Domestic Violent Extremist (DVE) Threats:

- DVE activity has increased nationwide but there are no current, credible threats to FEWAFB and the FEWAFB Missile Fields
- Anti-government DVE groups may wish to target MMIII and future Sentinel sites and construction activities, but likely view them as hard targets
- Lone offenders acting independently remain the primary actors in DVE attacks

Disinformation/Malign Influence Campaigns:

- Russia in particular has extensively used disinformation in the media (including social media) to attempt to turn public opinion against select U.S. military efforts
- No known disinformation campaigns targeting Sentinel but disinformation campaigns remain a threat, especially if targeting local populace

Protests:

- First Amendment-protected protests, politically-motivated vandalism may impede Sentinel-related construction; Most are non-violent and lawful



Disinformation Case Studies



Jade Helm Exercise (2015):

- Jade Helm was a U.S. military exercise involving 1,200 personnel designed to train soldiers to operate in overseas combat environments, including maneuvering through civilian populations
- Russia used a Facebook page to promote conspiracy theories claiming that the exercise was to lay the groundwork for martial law and mass internment
- Russia further promoted this conspiracy theory on English-language Russian media websites

5G Technology (2019 – 2020):

- Russian media promoted the conspiracy theory that 5G technology would give local personnel cancer and radiation
- Unknown vandals damaged 5G cell nodes in Texas on nine different occasions, rendering the nodes inoperable



DVE Threats to Infrastructure



Metcalf Substation Attack (2013):

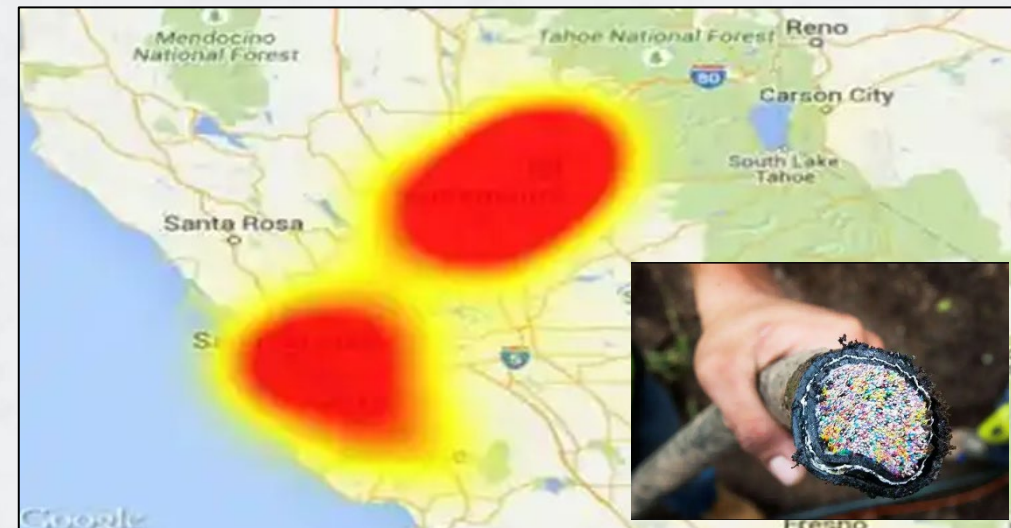
- Individual or small group attacked power substation with rifle fire
- Severe damage to 17 transformers, fiber optic cables also severed
- Direct impact minimal, but....

Bay Area Fiber Optic Cable Attacks (2014-2015):

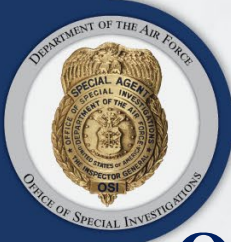
- At least 15 incidents of deliberately-severed fiber optic cables
- Some cuts affected Internet “backbone” fiber, emergency services

“Copycat” Attacks, Plots, Continuing Online Incitement

- September 2016 attack on transformer in south-central Utah
- Attacks on 5G cellular towers in 2020-2021
- December 2020 “SRVBIED” attack on network hub in Nashville
- DOJ investigating multiple plots to attack electrical infrastructure
- Online incitement by DVEs to attack electrical, comms facilities
- Varying beliefs, ideologies driving incitement: racist-extremist and anti-government “accelerationism,” conspiracy theories



Reportable Incidents



OSI requests your assistance in identifying and reporting:

- Purchases of land and/or real estate near Sentinel sites by foreign nationals
- New businesses near Sentinel sites owned and/or operated by foreign nationals
- New foreign cultural entities near Vandenberg SFB
- Any reported incidents of foreign nationals asking local personnel questions about missiles, MMIII, and/or Sentinel sites
- Foreign nationals known or suspected of conducting surveillance on or near Sentinel sites
- Suspicious activities near Vandenberg SFB and/or Sentinel sites
- Unmanned Aerial System (UAS) incidents near Vandenberg SFB and/or Sentinel sites
- Any aspirations or attempts to interfere with Sentinel construction by members of the local community
- Possible insider threats among the individuals working on Sentinel (military, civilians, cleared defense contractors, construction workers, etc)

Case Study: Russian SVR Illegal Donald Heathfield

Heathfield had a software business that he marketed to the U.S. military and DoD to as a guise to spot and assess possible sources. One individual was a U.S. government employee with information related to nuclear technology.

Office of Special Investigations

QUESTIONS?

