DOC DHS Space Cybersecurity Symposium III: NOAA/NESDIS Security Approaches

NOAA

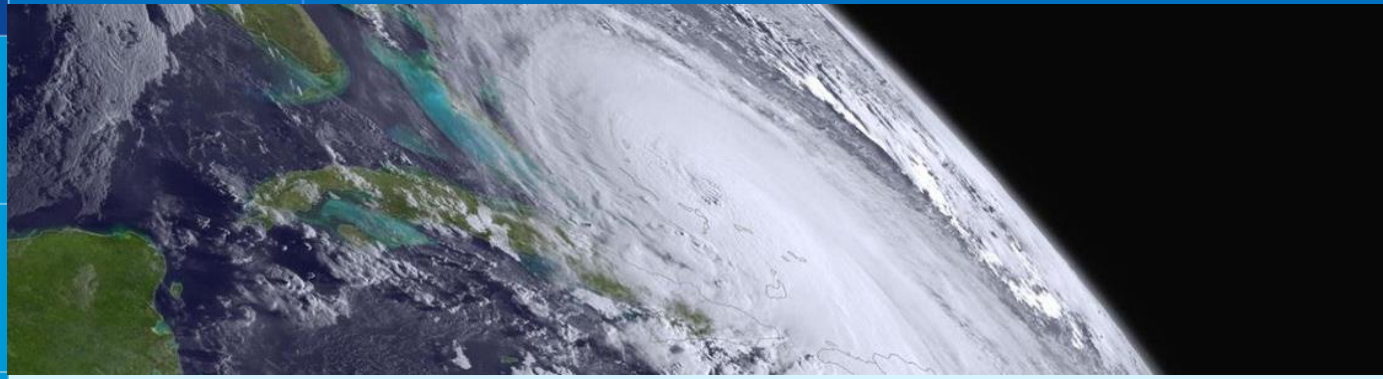
National Environmental Satellite, Data, and Information Service (NESDIS)

Presented by:

Manan Dalal

Assistant Chief Information Officer - Satellites

June 16, 2022



Agenda

- Threat landscape
- NOAA Business model & approach to threat landscape
- NESDIS Common Cloud Framework (NCCF)
- Operational Secure Ingest (OSIS)
- Supply Chain Risk Assessment (SCRA)
- Data Risk Assessment (DF-SCRA)
- Closing Remark & Questions

Future Threat Landscape

A number of recent security incidents across US government and commercial sector over the past few years have highlighted the risks from not understanding end-to-end supply chains of hardware and software. The nation relies on NOAA products to save lives and property. In many cases, these products integrate or use near-real time data acquired from International, non-governmental partners and the commercial sector. It is critical to understand and evaluate the risks associated with these data flows.

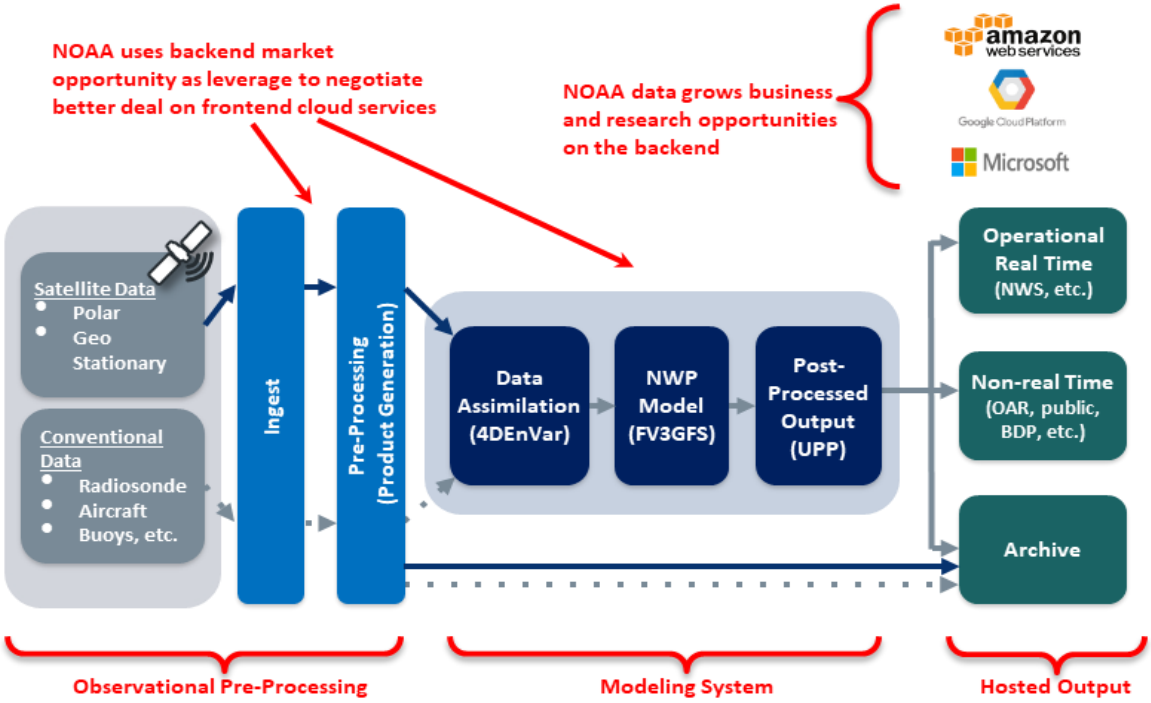
Examples of threats:

- Artificial intelligence (AI)/machine learning (ML) cyber attacks and the industry response for predictive cybersecurity
  - AWS Sqrrl procurement
  - Cylance AI antivirus
- Morphic Malware – customized AI created cyber threat software that is designed to attack a specific target
- Encrypted traffic malware goes undetected due to lack of deep packet inspection (DPI) technology utilization
- Internet of Things (IoT) distributed denial of service (DDOS) and botnet attacks

The best defense against such intelligent and automated threats is an integrated, collaborative, and highly adaptive security platform

NOAA Business Model

(Moving to the Cloud)

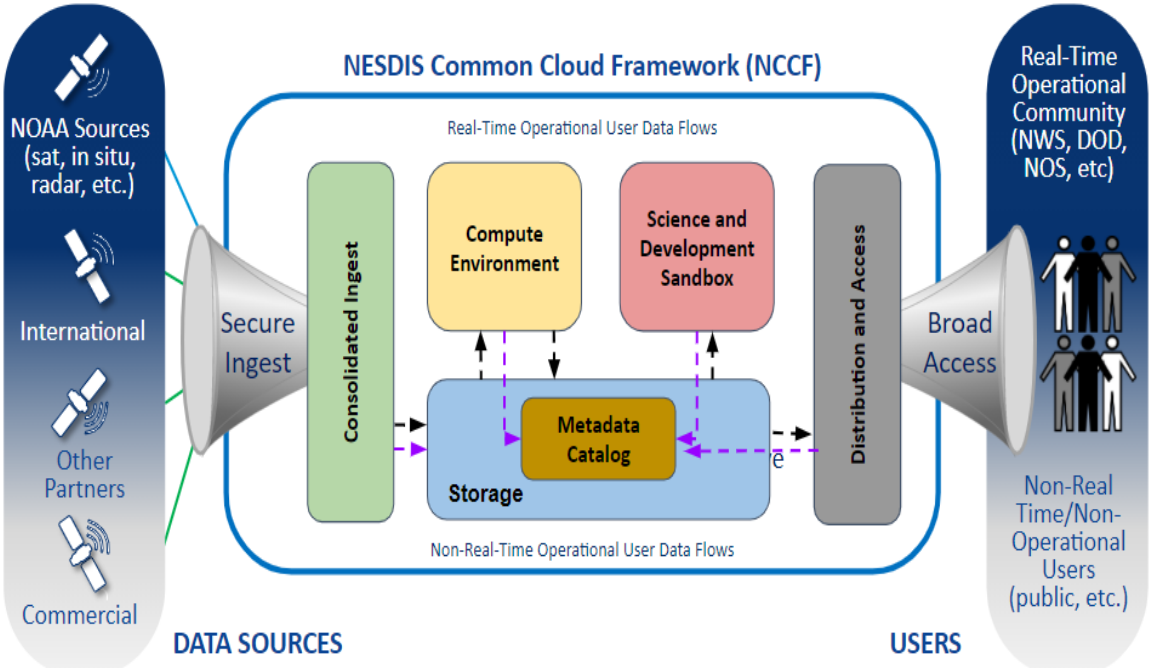


Approach to Address Business Needs & Threat Landscape

NESDIS has taken a multi-faceted approach, where we leveraged NOAA and DOC enterprise services, and developed line office unique services to address threats and business opportunities:

- Developed the **NESDIS Common Cloud Framework (NCCF)**
- Based on the NCCF - we developed an **Operational Secure Ingest Service (OSIS)**
- Leverage the DOC/NOAA **Supply Chain Risk Assessments (SCRA)**
- Developed a **Data-Flow Risk Assessment** (DF-SCRA) [classified & non-classified]

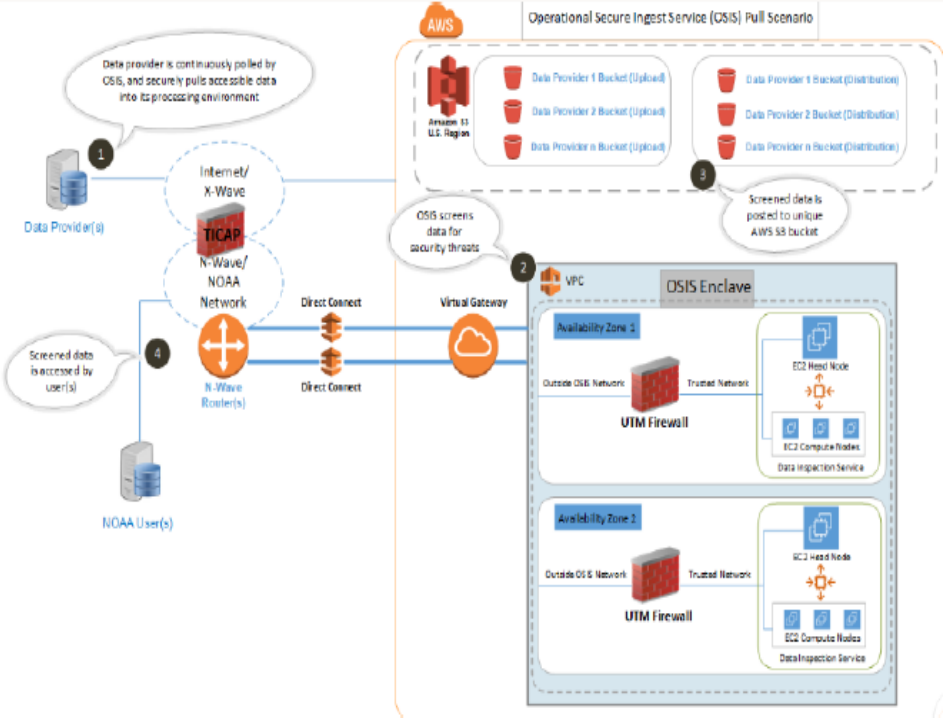
Solution for the Future



Operational Secure Ingest (OSIS)

Overview of Service:

- Cloud based service designed to monitor real time data ingests
- Use of AWS native tools
- TICAP and Anti-Virus
- AWS landing zones with associated controls
- Steganography scans to include science formats
- Operational 2020



Supply Chain Risk Assessment (SCRA)

NOAA Supply Chain Risk Management Program:

Evaluates and assess the supply chain risk from a presumptive company/vendor against available and relevant threat information to ensure the DOC/NOAA mission - while keeping NOAA systems secure

Key Components:

- Required for: i.) NEW High or Moderate FISMA system; ii.) Existing High FISMA systems; and iii.) System identified as a National Security System

  Or at the discretion key stakeholders (IT security professionals and senior NOAA leadership)

- Covers substantial, essential/critical technology of any system by a "covered foreign country"
- Does not include hardware such as cables, racks, stands, power cables, keyboards, etc.
- Not needed if a prior SCRM has been completed by another Federal agency

Data Flow Supply Chain Risk Assessment (DF-SCRA)

NESDIS Data-flow Supply Chain Risk Assessment Program:

Assessments to review the supply chain and data flow risk on operational data flows from non-NOAA data sources, including the US government, foreign government(s), commercial and non-Governmental Organizations - to ensure the mission while keeping NOAA systems secure.

Key Components:

- Examines source ownership; investors; insider threats; data flow pathways; transfer protocols; data type risks; data launching and landing location configurations
- Reviews both **open source** and **classified** information sources
- Assessment determination at the discretion of internal stakeholders: ranging from security professionals, Project/Program Managers and senior leadership
- Compares technical risks discovered against technical configuration of NESDIS systems
- Capable of reviewing foreign country agencies and their associated services

Closing Remarks

a) NOAA has a mature cybersecurity program that follows OMB, DHS, Department of Commerce and NIST rules, regulations and guidance to support the mission

b) NOAA/NESDIS works closely with cyber security experts at all levels to tailor programs to meet specific needs - from operational weather products, to flying spacecraft, to managing the Nation's climate data archive

c) Developed a cloud based zero trust architectural framework (NCCF) to support our end-to-end work-flows from ingest / processing / storage / access & dissemination / and achieve

d) NOAA/NESDIS is expanding into a new frontier of assessing risk of real time environment data feeds from foreign governments, non-governmental partners and the commercial sector using new cloud based technical means, as well as old-fashioned research using open source and classified means

e) All Federal agencies need to develop mechanisms to better enable the sharing of vendor risk data (SCRA, data risk, etc.) to better protect our missions

Questions