NICS Frequently Asked Questions

What is NICS?

NICS is a ***mobile, web-based*** command & control environment for dynamically escalating incidents from ***first response*** **to** ***extreme-scale*** that facilitates collaboration across Federal, Tribal, Military, State, County, Local/Municipal, and Utility levels of preparedness, planning, response, and recovery for ***all-risk/all-hazard*** events.

NICS is designed to develop and nurture situational awareness, particularly for those at the point of the sword looking directly at the threat.

NICS is:

- Open Standards
- Community effort
- Non-proprietary
- Scalable
- Rooted in ICS

NICS can be thought of as a "product" that is "on the market," but more accurately it is a "*set of tools and technologies that are provided at no cost to all emergency response organizations, and which are in continued development and maturation via the development of plug-and-play apps*" where anyone can develop and submit an app for inclusion into NICS (operators, researchers, small and large companies, academia, government labs, etc.).

What is the goal of NICS?

The goal of NICS: Develop and provide technology for the **Tired – Dirty – Hungry** responder under extreme stress.

Dirt-simple-to-learn and dirt-simple-to-use.

If a new user knows how to turn on a computer, knows how to surf the web, and can find the neighborhood Olive Garden using Google Maps, then they can learn everything there is to know about NICS in 60 minutes or less.

How is NICS different from other approaches?

Primarily (but not exclusively) visually based rather that text based
Aimed at the Tired – Dirty – Hungry
Uses an Apps Model for growth, expansion, and tailoring of NICS; anyone can develop an app
Provided at no cost to all emergency response organizations

Who is developing NICS tools and technologies?

NICS was conceived, envisioned, and functionally specified by experienced first responders, many from the California emergency response community, and developed by skilled scientists and engineers at the Massachusetts Institute of Technology Lincoln Laboratory (MIT LL), an FFRDC at Hanscom Air Force Base in Bedford, MA.

What is an FFRDC?

An FFRDC is a Federally Funded Research and Development Center that conducts research for the Federal Government. Currently there are 39 in the United States. FFRDCs typically assist government agencies with scientific research and analysis, systems development, and systems acquisition. As they are funded by the government, they can be thought of as government laboratories. Many are associated with prominent universities, and professors and staff can migrate from the center to the campus as justified by research interests and needs. See http://www.nsf.gov/statistics/ffrdclist/ for a current list of FFRDCs and their sponsors.

MIT Lincoln Laboratory: MIT LL (see: http://www.ll.mit.edu/) is an FFRDC associated with Massachusetts Institute of Technology that applies advanced technology to problems of national security. Research and development activities focus on long-term technology development as well as rapid system prototyping and demonstration. These efforts are aligned within key mission areas: Space Control, Air & Missile Defense Technology, Communications Systems, Cyber Security & Information Sciences, ISR Systems & Technology, Advanced Technology Development, Tactical Systems, Homeland Protection, Air Traffic Control, and Engineering. The Laboratory works with industry to transition new concepts and technology for system development and deployment.

MIT LL has its primary research facilities at Hanscom Air Force Base in Bedford, MA. Its staff includes 3,500 scientists and engineers.

Who has funded the NICS development?

MIT LL (http://www.ll.mit.edu/) funded the initial phase of NICS development (2007-2010).

The Department of Homeland Security (DHS) Science & Technology Directorate (S&T) (http://www.dhs.gov/st-organization) funded the second phase (2010-2014).

Additional funding was provided in 2013 by the County of San Diego, San Diego Gas & Electric (http://www.sdge.com), and the U.S. Coast Guard.

Is NICS Intellectual Property owned by a vendor? Is any part of NICS proprietary?

NICS is an open community project. No part of NICS is proprietary. No NICS intellectual property is owned by a vendor.

What are the guiding design principles for NICS development?

NICS development is guided by eight design principles:

1) Adherence to the principles and operation of the Incident Command System (ICS)

2) Seamless scalability (from initial dispatch through extreme scale events)

3) Network to the edge (connect those at the point of the sword)

4) Technology neutral (works with any device, any operating system, any browser)

5) App store approach for growth, expansion, and tailoring

6) All hazard/all risk

7) Focus on the Tired – Dirty – Hungry

8) Provided at no cost to all emergency response organizations

How well does NICS scale? What are the goals?

NICS is intended to scale to 1000s of responders from 100s of organizations working dozens of incident at the same time. To date, NICS has been stress tested with up to 150 simultaneous users. (More below)

Can NICS support multiple incidents? If so, how many?

NICS can and has supported multiple incidents with scores of users from dozens of organizations. To date an upper bound has not been reached. As the user base grows, performance will be continually assessed in order to benchmark scalability.

What computers/devices, operating systems, and browsers does NICS work on?

NICS can run on any web-capable computer or device using any operating system.

NICS works on all browsers except Internet Explorer Version 8 and earlier. It works on Internet Explorer Version 9 and later. It also works on FireFox, Chrome, Safari, and others.

Tablets & Smart Phones: NICS works on any computers or devices that can run these browsers. Regarding Tablets and Smart Phones, The US Coast Guard (USCG) has funded mobile Tablet and Smart Phone apps for NICS. The Android app is complete and authorization to disseminate it is imminent. The iOS app is still under development and is expected to be complete by the first quarter of 2014.

Who funded the hosting of NICS at the San Diego Supercomputer Center?

The San Diego Supercomputer Center operation of NICS was funded by the San Diego County Board of Supervisors under the leadership of Supervisor Ron Roberts. This site is available for all responders using NICS.

Will DHS provide hosting services for NICS in the future?

DHS is not interested in hosting NICS since NICS is being used primarily for real operations supporting actual emergency responders across the U.S., as opposed to use by the DHS Components. A similar discussion with the National Guard raised the concern that first responders would not be able to access military networks.

What is the current server physical distribution? Where are the primary and backup servers? What is the plan for future distribution of NICS servers?

In 2013, the runtime instance of NICS was moved from the servers at MIT LL (Hanscom AFB, MA) to the servers at the San Diego Supercomputer Center on the campus of the University of California at San Diego. This was the first test of using a conventional host outside of the MIT LL R&D server farm.

Part of the research objectives of NICS is to test and assess different configurations of servers and back up systems to achieve maximum resiliency during catastrophic events. It is believed that any top tier server facility can suitably host NICS (e.g., Rack-Space, Amazon, etc.).

Evaluation of server configuration and physical siting will help define and validate an elastic operating environment: Multiple dispersed physical locations for maximum survival in case of regional disasters; low cost crowd configurations; out-of-country sites where appropriate.

How much computation is required to run NICS? How much Internet capability?

NICS is a conventional Web application. It can run on any adequately configured computer, even a laptop.

The San Diego Supercomputer Center, as the current host for NICS, has a number of powerful super computers for research purposes but NICS does not use any of these or require them for its performance. It runs with very modest demands on the Center's basic server infrastructure. If needed, NICS could be run off of a suitably powered commercial laptop.

The NICS operators have conducted "stress tests" of NICS with 50 and 150 user exercises that drive NICS tools and technologies as hard as possible.

For example, one test has all users simultaneously draw graphics, place symbols, and create text labels as fast as they can from multiple remote locations. This is many times greater (x100? x500? x1000?) than the typical load that has been observed during real incidents.

NICS has performed without decrement during each of these tests. Furthermore, MIT LL conducts periodic scalability evaluations using an elastic cyber-range test bed; effectively, hundreds or thousands of emulated users are created in "the cloud" to identify stress points.

Is NICS HTML 5 compliant?

NICS is HTML 5 compliant. However, not all web browsers support full HTML 5. This is particularly true for some mobile browsers.

What is the NICS Users' Group?

The NICS User's Group is a volunteer organization of all NICS registered users and interested parties that has assumed incident command of the transition process for NICS.

How well does NICS work with satellite communications?

NICS does not work well over BGAN. This is not strictly a bandwidth problem, but rather a 'delay' problem. TCP/IP requires acknowledgements per packet, and re-transmits if the packets aren't received in time.

Performance Enhancing Proxies (PEPs) can mitigate this issue somewhat. The bulk of bandwidth is consumed during login – one CONOPs could be to login to NICS on a decent comm connection, put the computer to sleep, and then re-open the computer over the satcom.

NICS will automatically re-connect without having to re-login. This isn't particularly suited to the Tired – Dirty – Hungry design principles of NICS, but could help.

DHS S&T commissioned MIT LL to conduct a study: "A Review of Satellite Communications and Complementary Approaches to Support Distributed Disaster Relief" that they are preparing to release that adds further light to this question.

How does NICS handle reports and data management used in the Incident Command System?

There are a number of forms, spreadsheets, and other ICS-based tools that are in the development pipeline, many which will dramatically streamline and improve the efficiency of information sharing and commander collaboration during incidents.

Work sponsored by the USCG will introduce additional forms pertaining to operational periods and resource tasking. Follow-on work will be funded to incorporate additional ICS forms and reports in FY14. There is a long list of items, features, and capabilities prioritized for development and implementation into NICS. This list can be provided upon request.

Security

User Certification

Anyone can request a NICS account, but a NICS administrator from that user's First Responder organization must approve the account before the new user can access the system. The NICS Users' Group is responsible for approving new organizations' participation.

User Roles

NICS user roles are defined here: http://public.nics.ll.mit.edu/nicshelp/articles/usergroups.php

Essentially a user can be given read only, read & write, and various administrative privileges.

During actual incidents, user roles can be managed depending upon the duties of the user. Some users can be denied or granted access to specific collaboration rooms or specific data.

Usernames

Usernames are email accounts. Currently there is a business process put in place by the NICS Users' Group to only allow .gov, .mil, and in some cases .edu accounts.

There have been some exceptions (Red Cross, Utility companies, etc.), but they must be approved by the Users' Group. Some legacy users still use non-email usernames; these will eventually be migrated to their email accounts.

Passwords

Users create their own passwords, which are encrypted (MD5 hash) and stored in the database. Users can change their passwords at any time and request a password reminder via email.

Server Encryption

NICS uses bank/military grade SSL certificates (256-bit AES encrypted HTTPS + SSL (TLS)) on the "Incident" server.

Next Level Security

NICS is introducing a new security layer powered by OpenAM to further protect the system. See: http://forgerock.com/what-we-offer/open-identity-stack/openam/

Protection of Data Feeds

Some incoming Position Location Information (PLI) and/or Automatic Vehicle Location (AVL) data (i.e., tracking) comes over secure VPN connections using an ASA firewall.

Other feeds use encrypted channels. Still others are not encrypted. NICS can support these modalities. The selection is usually determined by the Data Provider based upon their capabilities and the sensitivity of the data. Once the data is received by NICS, it can only be

accessed on the "Internet" via the web.

Only authenticated NICS users can access these feeds through NICS. There's also an ability to protect a data feed using a password to further limit access.

Some Questions Relating to Using NICS With Power/Water/Gas Utility Providers

Q: Are the following alternatives to accessible data layers feasible? Are there any other alternatives? Can an enabling utility push a data layer of assets for a limited geographic area onto NICS when an emergency arises in that area? (For example, a fire breaks out in the Santa Cruz Mountains and then San Jose Water company and PG&E make data layers available that show substations, transmission lines, reservoirs and pumping stations for the impacted region only.)

A: The Data Provider initiates the sharing action and sends data to the secure NICS server. The Provider controls what, when, and for how long specific data is sent to the secure NICS server. NICS is able to receive static data files (e.g., KMZ, KML, and Shape formats) or dynamic data layers (e.g., WMS, WFS, ArcGISRest, etc.).

The static data resides on that server until it is deleted by the Data Provider or other designated agent. Similarly, dynamic data links are available until they are removed by the Data Provider or other designated agent.

This data can only be viewed but not copied.

Q: Can data layers be password protected and only be activated by the utility Incident Commander?

A: If the Data Provider is hosting the data, NICS supports HTTP Basic Authorization and ArcGIS Tokens to exchange username/password information in order to make data available to Provider approved users.

Currently, NICS does not support creating data layer specific usernames and passwords for NICS hosted data, but this feature is on the development list and will be completed in the next several months. This capability was suggested by SDGE.

Q: The above scenarios are contingent on the utilities being able to shut off or remove the data layers after the incident is completed. Is that possible?

A: Yes. Deleting data or shutting off data can be done at any time by the Data Provider or designated agent whenever the data is no longer necessary.

Q: How is NICS currently protected from cyber security threats? How is system security currently

monitored?

A: There are three levels of system monitoring and protection:

- Network Level: MIT Lincoln Laboratory (MIT LL) constantly monitors all network traffic for anomalies, and alerts are issued immediately if a suspected issue is identified.

- Systems Level: All NICS systems are constantly monitored for any unusual performance, and alerts are sent if an issue is identified.

- Application Level: Server encryption is described above as is user access certification. Data Provider's data is controlled by the Provider (what, when, and how long) and copies of Provider's data are not made. Once deleted, it is deleted.

  MIT LL also conducts periodic intrusion detection to identify any system vulnerabilities.

Q: How is WebEOC the same or different from NICS? Could NICS become the plug-in that replaces the current WebEOC map feature?

A: WebEOC is installed in a large number of command centers and recognized by CAL OES as the EOC level tool for information gathering, sharing, and dissemination.

WebEOC is a text-oriented information-sharing tool: text reports (typically a paragraph or two, a "sit-rep" or situation report to use a military term) flow into the EOC and are routed to the function that it is addressed to (e.g., a report on a highway closing would go to the Transportation Desk).

As such, WebEOC is an office-to-office tool. It is not designed to be used at the front line where responders are dealing with an incident face-to-face.

Because each EOC has its own version and runs WebEOC on its own servers, standardization between organizations is a continual issue.

WebEOC has weak visualization and mapping tools.

NICS derives it strength through strong, easy to use visualization and mapping tools designed to be used by the Tired – Dirty – Hungry responder under extreme stress.

NICS can cut-and-paste text from WebEOC into NICS ICS reports (e.g., the Report On Conditions; the 215 report) as well as attach text, images, and video to graphics and symbols.

In this way, NICS and WebEOC are complementary and can work together. Work is underway to integrate these two tools.

An initial demonstration of data exchange between NICS and WebEOC has been performed, although additional work is required before this capability can be used operationally.

Regarding NICS replacing the map feature in WebEOC: NICS data could flow into WebEOC, although it hasn't been demonstrated yet. This is not due to any technical restrictions, but there have been some questions around WebEOC's licensing and whether it was

permitted for NICS data to flow into the system. ESI had previously advised against it, but we've also spoken with user organizations who say it's OK. Due to the ambiguity, we have refrained from pursuing it.

Finally, NICS is provided at no cost to emergency responders. WebEOC is not.

Current Programmatics:

DHS S&T funding concludes in FY14 consistent with their policy to fund projects only for a limited period. A program plan to continue NICS development, fielding, and testing has been prepared and is available for review and comment. The NICS team is seeking sponsor(s) for the next 5-year phase of development.