

National Open Source Strategic Action Plan

Department of Homeland Security
Federal Bureau of Investigation
United States Army
National Security Agency
National Virtual Translation Center

Department of State
United States Marine Corps
Director of National Intelligence Open Source Center
Defense Intelligence Agency

Central Intelligence Agency
United States Air Force
United States Coast Guard
National Geospatial-Intelligence Agency
Drug Enforcement Administration

United States Navy

FY09

Chairman's Message

I am pleased to present the National Open Source Committee's "Strategic Action Plan" for FY2009. While the emphasis is on action—specific goals and objectives for FY09—the document also provides the strategic context and drivers for these objectives.

The NOSC is entering a new phase in its evolution as bridge between strategy and implementation. Proceeding from the vision and goals initially laid out in the 2006 "National Open Source Enterprise," the NOSC is now narrowing the aperture to focus on those areas that will maximize benefit to the larger open source enterprise while facilitating the work of those who are developing their open source capabilities. As with any joint venture, the success of our enterprise will depend on the unique attributes its members bring to bear. Our job is to develop those attributes while working together to ensure they are put to the broadest possible use—for the benefit of the larger enterprise and, more important, for those who make US national security policy and defend our nation.



Douglas J. Naquin
Chairman, National Open Source Committee
Director, DNI Open Source Center



Vision

Open sources are integral to the planning, execution, and success of all US national security initiatives.

Mission

To facilitate the effective application of the nation's collective open source capabilities in support of national security.

Values

Integration: The impact of open source information is most evident when it is combined with other collection disciplines to inform in ways that are unique, timely, and cost effective.

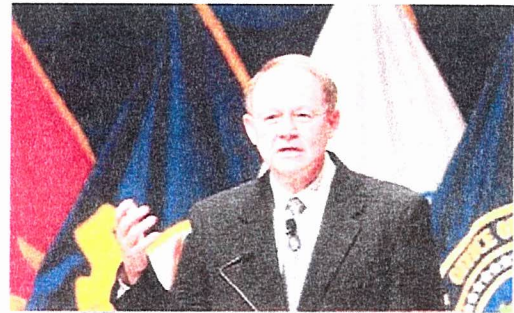
Collaboration: The open source enterprise transcends organizational boundaries to connect capabilities and expertise on issues of common concern, as well as to combine our capabilities with those of the larger national security community.

Transparency: The more we know about our collective capabilities and needs, the better decisions and recommendations we will make.

Continuous improvement: We facilitate the work of those who support the enterprise by establishing, measuring, and improving processes that enable their success.

Realizing the “National Open Source Enterprise”

The DNI’s articulation of the National Open Source Enterprise in 2006 represented a critical step in formalizing the vital role open sources play in achieving “decision advantage.” By acknowledging open source exploitation as a foundation for all intelligence disciplines, the DNI placed a spotlight on a discipline of vast but underrated potential. To nurture this new enterprise, the National Open Source Committee (NOSC)—a body of partners representing the intelligence, defense, diplomatic, and homeland security domains—was formed to serve as a bridge between strategy and implementation. Its primary roles are to facilitate the work of those who are building open source capabilities and expertise and to ensure the results of this work feed back into the larger open source—and intelligence—enterprises.



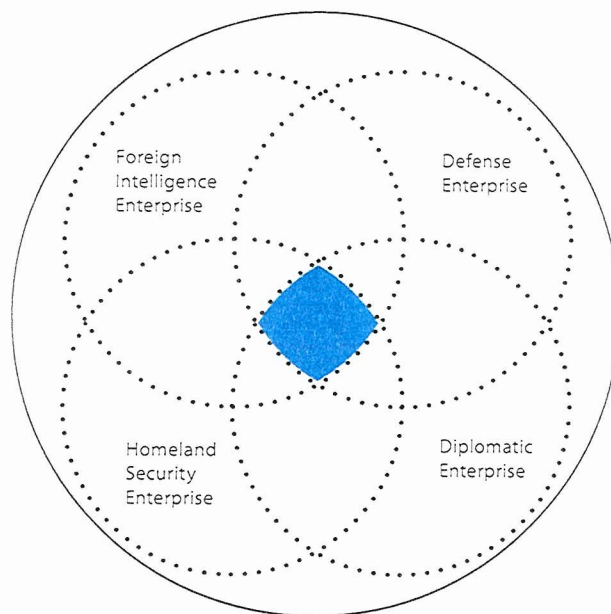
Director of National Intelligence, Mr. Mike McConnell.
Source: AP

“No aspect of collection requires greater consideration or holds more promise than open source information.”

—DNI Vision 2015

As we enter FY2009, we still face the challenge of moving open source from afterthought to integral in intelligence, defense, and homeland security strategic planning and implementation. To this end, the “Open Source Enterprise” must focus on integration—both among the capabilities that exist within the open source community and between the collective open source and the broader intelligence enterprises. These fundamental tenets are highlighted in the Intelligence Community’s *Vision 2015—A Globally Networked and Integrated Intelligence Enterprise* and reflected in our goals and objectives for 2009 and beyond.

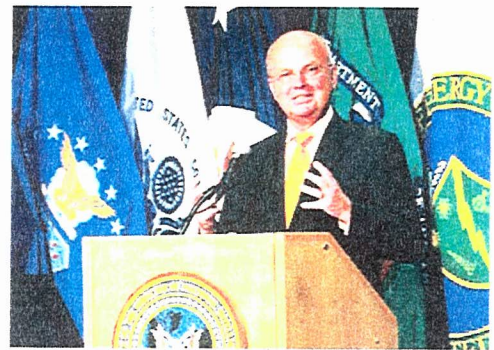
As the Open Source Enterprise and NOSC have matured, we have also come to realize our “enterprise” is not monolithic, whereby one approach must meet the needs of all (or all must adjust their needs to accommodate one approach). In fact, the “National Open Source Enterprise” is more accurately an “enterprise of enterprises” with separate but interlocking domains for foreign intelligence, defense, homeland security, and diplomacy, each driven by unique missions and policies. The National Open Source Enterprise’s goal is to focus on the “sweet spot” where the four domains intersect and then to expand that “sweet spot” through collaboration and the sharing of people, tradecraft, and technology.



National Open Source Enterprise

Second, while the NOSC is committed to collaboration and integration across the National Open Source Enterprise, integration with the larger national security domain—comprising all collection disciplines and all-source analysis—is of equal or greater importance. NOSC integration efforts, therefore, will focus as much on cross-discipline integration as on intra-open source integration.

Third, we cannot lose sight of our ultimate goal—impact. The processes we create, architectures we sponsor, integration we facilitate, expertise we develop, and resources we invest all aim to bring new and improved value to those who make and execute US national security policy. Those who have worked in and with the open source domain over the past few years cannot help but marvel at the dynamism of the open source environment and potential it offers for “decision advantage.” We look forward to unleashing this potential for unprecedented benefit.



Director, Central Intelligence Agency
Mr. Michael Hayden

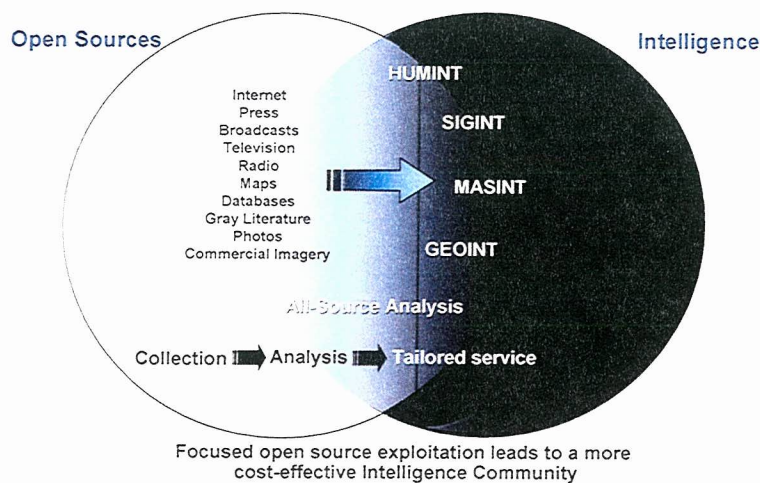
“Open source intelligence is widely seen as both an essential capability and a formal asset in our national security infrastructure.”

*—DCIA Michael Hayden
DNI Open Source Conference
September 2008*

The goals and objectives outlined herein represent an important step—not only in making tangible progress within the National Open Source Enterprise, but in the broader community’s commitment to work together to realize a vision of using our collective capabilities toward a common purpose.

Our Goals

- **Universal, cross-domain (Top Secret, Secret, Unclassified) access:** We enable the broadest possible access to open source data, products, and services and support discovery, search, and collaboration in our customers' preferred work domains.
- **Integrated mission management and impact:** Open source is integral to all-source strategies and used to its maximum potential in informing those who make and execute national security policy.
- **Proliferation of open source expertise:** Open source exploitation is prevalent throughout the national security community, and embedded open source specialists apply unique expertise in support of their respective organizations' missions.
- **Open Source Enterprise governance:** Our governance ensures alignment with DNI priorities, informs decision-making, and facilitates the effective application of the national security community's collective open source capabilities.



Our Objectives

1. Universal, Cross-Domain Access

- 1.1 In concert with DNI/CIO, develop an enterprise architecture conducive to making open source data and products as widely available as possible.
- 1.2 Increase access to currently available open source products and services on both unclassified and classified domains.

2. Integrated Mission Management

- 2.1 Develop and implement a process for providing enterprise-wide open source responses to substantive DNI taskings (e.g., NIC-C, NIC-B).
- 2.2 Achieve initial operating capability for the open source collection requirements management and tasking system—OSCaR-MS.
- 2.3 Increase the number of “enterprise partnerships”—USG, foreign liaison, academia, and/or commercial— for community benefit.
- 2.4 Identify “centers of excellence” upon which the Open Source Enterprise can depend for unique products or services or economies of scale.
- 2.5 Develop an integrated open source resource plan in support of DNI and Open Source Enterprise priorities.
- 2.6 In response to DNI priorities, identify and provide unique content for community exploitation.
- 2.7 Reach full operating capability for the Integrated Linguist Activity-Doha.
- 2.8 Develop a strategy and resource plan to grow foreign language processing capacity (e.g., translations, language processing technology).
- 2.9 Enable the development and implementation of the Department of Homeland Security’s Domestic Open Source Enterprise.

3. Proliferation of Open Source Expertise

- 3.1 Establish an open source curriculum (or curricula) to be embedded in introductory training programs offered by agencies and components throughout the national security community.
- 3.2 Develop an open source training taxonomy and course catalog that can be accessed throughout the Enterprise.
- 3.3 In concert with DNI/CHICO, establish core competencies for open source specialists for application throughout the Enterprise.
- 3.4 Increase the number of open source specialists/practitioners embedded in mission elements.
- 3.5 Develop a plan to provide open source training on-line.

4. Enterprise Governance

- 4.1 Revise the governance structure to improve insight, inform decision-making, and facilitate the accomplishment of the above goals and objectives.
- 4.2 Increase insight into open source-specific resources across the Enterprise.

“The Open Source Board of Governors...will set direction and priorities in a way that allow each of the players, each of the elements of the Open Source Enterprise to develop and make the most of their capabilities.”

*–DCIA Michael Hayden
DNI Open Source Conference
September 2008*

Department of Homeland Security
Federal Bureau of Investigation
United States Army
National Security Agency
National Virtual Translation Center

Department of State
United States Marine Corps
Director of National Intelligence
Defense Intelligence Agency

Central Intelligence Agency
United States Air Force
United States Coast Guard
National Geospatial-Intelligence Agency
Drug Enforcement Administration

United States Navy
Open Source Center

FY09