

# Space-Based Domestic Spying: Kicking Civil Liberties to the Curb

By [Tom Burghardt](#)

Global Research, November 09, 2008

[Antifascist Calling](#) 9 November 2008

Region: [USA](#)

Theme: [Police State & Civil Rights](#)

Last month, I [reported](#) that the Department of Homeland Security's ([DHS](#)) space-based domestic spy program run by that agency's National Applications Office (NAO) had gone live October 1.

Federal Computer Week [reports](#) that Charles Allen, DHS' Undersecretary for Intelligence and Analysis, told the 5th annual [GEOINT Symposium](#) on geospatial intelligence in Nashville late last month that, "DHS' imagery requirements are significantly greater, in number and scope, than they were at the department's creation, and will continue to grow at an accelerating rate as the department's mission-space evolves."

Indeed during Hurricane Ike, U.S. Customs and Border Protection for the first time flew the Predator B unmanned aerial vehicle in "support of the Federal Emergency Management Agency's relief efforts," the insider tech publication reported.

As readers are well aware, the Predator B carries out "targeted assassinations" of "terrorist suspects" across Afghanistan, Iraq and Pakistan. The deployment of the robotic killing machines in the United States for "disaster management" is troubling to say the least and a harbinger of things to come.

Despite objections by Congress and civil liberties groups DHS, in close collaboration with the ultra-spooky National Reconnaissance Office ([NRO](#)), the agency that develops and maintains America's fleet of military spy satellites, and the National Geospatial-Intelligence Agency ([NGA](#)) that analyzes military imagery and generates mapping tools, are proceeding with the first phase of the controversial domestic spying program.

NAO will coordinate how domestic law enforcement and "disaster relief" agencies such as FEMA will use satellite imagery intelligence (IMINT) generated by military spy satellites. As I [wrote](#) earlier this year, unlike commercial satellites, their military cousins are far more flexible, have greater resolution and therefore possess more power to monitor human activity.

Testifying before the House Homeland Security committee in September, Barry Steinhardt, Director of the ACLU's Technology and Liberty Project, called for a moratorium on the domestic use of military spy satellites until key questions were answered. Steinhardt [said](#), "Congress needs to act before this potentially powerful surveillance tool is turned inward upon the American people. The domestic use of spy satellites represents a potential monster in the making, and we need to put some restraints in place before it grows into something that will trample Americans' privacy rights."

Needless to say, a feckless Congress has done virtually nothing to halt the program. As The Wall Street Journal [reported](#) in early October, Congress' "partial funding" of the office "in a little debated \$634 billion spending measure," means that NAO is now providing federal, state and local officials "with extensive access to spy-satellite imagery."

Allen told the GEOINT Symposium that while "geospatial efforts are being coordinated across agencies," technical hurdles must be overcome in order to improve geospatial IT applications. Federal Computer Week avers,

For developing future satellite imagery capabilities, Allen recommended diversity, availability, survivability and flexibility for future systems in a satellite and modular payload system similar to what was advised by the Marino Report in July 2007 to the director of the National Geospatial-Intelligence Agency and the National Reconnaissance Office.

"It describes an architecture that allows for short time between launch as well as an option for variable modalities. This kind of diversity is what I believe will be necessary to assure adequate collection of a wide array of targets," Allen said. (Alice Lipowicz, "Geospatial Intelligence Use Grows at DHS, Official Says," Federal Computer Week, October 30, 2008)

What those "variable modalities" are were not spelled out by Federal Computer Week. However, the Marino Report was released by [Chesapeake Analytics Corporation](#), an under-the-radar Arlington, Virginia-based private defense contractor that describes itself "as a 'boutique' consulting firm" for senior executives "in the geospatial technology sector." The [report](#) itself was written by Defense Group Inc. ([DGI](#)), a spooky Falls Church, Virginia defense contractor for NRO and NGA. According to their website, DGI "customers" include the Department of Homeland Security, the Department of Defense and "numerous Intelligence Agencies."

As we have seen however, the use of satellite imagery during "national security events" such as last summer's political conventions in Denver and St. Paul may have aided FBI and local law enforcement in their preemptive raids on protest organizers and subsequent squelching of dissent. One wonders if this is what DGI refers to when they write that the company "performs work in the national interest, advancing public safety and national security through innovative research, analysis and applied technology"?

NAO's launch is all the more troubling since an independent review of the program by the Government Accountability Office ([GAO](#)) found that the department has been less than forthcoming that NAO complies with privacy laws and doesn't violate the Posse Comitatus Act.

The 1878 law prohibits the military from playing a role in domestic law enforcement. Since the 1990s however, Posse Comitatus has been eroded significantly by both Democratic and Republican administrations, primarily in the areas of "drug interdiction," "border security" as well as "Continuity of Government" planning by U.S. Northern Command (NORTHCOM).

Despite objections by GAO auditors DHS securocrats held up the release of their 60-page report, citing its "sensitive nature." The September 15, 2008 [report](#), entitled "National Applications Office. Certification of Compliance With Legal, Privacy, and Civil Liberties Standards Needs to Be More Fully Justified," is now in the public domain and was finally released November 6, two days after American national elections.

It makes for a very troubling read. In their November 6 cover letter to congressional committees, the GAO writes:

*Citing a growing need to use classified satellite information for civil or domestic purposes, in 2005, an independent study group reviewed the future role of the CAC [Civil Applications Committee] and concluded that although the civil domestic users were well supported through the CAC, homeland security and law enforcement users lacked a coherent, organized, and focused process to access classified satellite information. (GAO, "National Applications Office Certification Review," GAO-09-105R, November 6, 2008)*

However, the "independent study group" cited by GAO was either independent nor predisposed towards limiting the deployment of military spy satellites for domestic "missions." Indeed that report, "Independent Study Group, Civil Applications Committee Blue Ribbon Study," (September 2005), was the product of a panel comprised solely of securocrats and defense and security contractors who stand to make a bundle on NAO. As investigative journalist Tim Shorrock [revealed](#) last year, the intelligence-sharing system to be managed by NAO,

*...will rely heavily on private contractors including Boeing, BAE Systems, L-3 Communications and Science Applications International Corporation (SAIC). These companies already provide technology and personnel to U.S. agencies involved in foreign intelligence, and the NAO greatly expands their markets. Indeed, at an intelligence conference in San Antonio, Texas, last month, the titans of the industry were actively lobbying intelligence officials to buy products specifically designed for domestic surveillance. ("Domestic Spying, Inc." CorpWatch, November 27, 2007)*

Indeed, the "independent study group" was appointed by Mike McConnell, the Director of National Intelligence who himself was a senior vice president for ten years with the spooky Booz Allen Hamilton corporation. McConnell oversaw that firm's extensive contracts in military intelligence and information operations for the Pentagon, Shorrock [reported](#) in March 2008.

GAO investigators have determined that while DHS "has established procedures for legal review, it has not yet fully addressed all outstanding issues regarding how the planned operations of the NAO, as described in the department's certification documents, are to comply with legal requirements. Specifically, DHS has not resolved legal and policy issues associated with NAO support for law enforcement." As investigators outlined:

DHS originally did not fulfill agency requirements to identify privacy risks and control mechanisms but recently has taken steps to do so. At the time of NAO certification, DHS did not fully explain how the office would comply with widely accepted privacy standards, such as the need for personally identifiable information to be accurate, secure, and used only for limited purposes. Specifically, the NAO's original privacy assessment did not identify or analyze the risks that NAO operations might not meet these standards, nor did it specify measures to mitigate such risks. In response to discussions with us regarding these shortcomings, the Privacy Office developed a revised assessment that represented a substantial improvement in identifying privacy risks and mitigating controls to address them, such as providing appropriate oversight and building a process to identify and correct inaccurate information. However, differences between the review procedures outlined in the revised privacy impact assessment and those in the standard operating procedures raise questions about whether the specifics of the NAO's privacy protection controls have been

clearly established. (GAO, op. cit. p. 4)

While paltry recommendations towards mitigating potential civil liberties' and privacy abuses by NAO were submitted to the DHS Undersecretary of Intelligence and Analysis (Charles Allen), GAO found that "specific measures have not yet been developed to address the potential for improper use or retention of information provided by the NAO and the potential for impermissible requests to be accepted as a result of a reliance on broad annual memorandums as justifications." In other words at NAO, as at other intelligence agencies across the war on terror's domestic "battlespace," it's business as usual.

Three categories of classified satellite information are to be provided law enforcement by the National Applications Office:

\* Geospatial intelligence (GEOINT)-GEOINT is defined as "the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information."

\* Measurement and signature intelligence (MASINT)-MASINT is defined as intelligence "derived from measurements of physical phenomena intrinsic to an object or event." These phenomena can include the following types: "electro-optical, infrared, laser, spectral, radar, polarimetric, high-power or unintentional radio frequency emanations, geophysical, chemical, biological, radiological, or nuclear."

\* Electronic intelligence (ELINT)-ELINT is defined as "technical and geolocation intelligence derived from non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. It does not include oral or written communications." Thus, ELINT could include intelligence based on signals from machines, such as computers, but not telephone conversations or other communications between individuals. (GAO, op. cit., p. 25)

While DHS has yet to resolve legal and policy issues associated with NAO support for law enforcement operations, the Office still continues to identify such support as a key element of its "mission." Indeed, DHS' Civil Rights and Civil Liberties Office did not resolve how NAO will comply with the applicability of the 4th Amendment to the Constitution which prohibits unreasonable searches and seizures, Posse Comitatus and the Reagan-era Executive Order 12333 that limits how federal intelligence agencies collect information on U.S. citizens and legal residents.

Citing lax standards in NAO's legal review process, GAO found that "the process for developing and approving annual memorandums for MASINT and ELINT has not been delineated. Such procedures are an important control in assuring that access, retention, and sharing of information is properly constrained."

However, as the eight long years of the Bush administration have demonstrated, any and all measures to "constrain" out of control federal spy agencies and their privatized assets in the corporate world have been rebuffed. Indeed, congressional oversight of the "intelligence community" and the Executive Branch is a joke-at the expense of an informed citizenry and democratic institutions accountable to the American people.

While DHS claims that data gathered for law enforcement purposes will be "in compliance

with privacy and civil liberties laws and policies of the United States,” the GAO found that “by broadly sharing information with non-federal users, who are not bound by the Privacy Act, personal information could be at risk of being used in ways not specified when it was originally collected.” Considering that some 70% of U.S. intelligence assets are employees of private security and defense contractors, NAO is a civil liberties disaster waiting to happen.

GAO identified four key areas where privacy risks have been identified:

1. An individual may be unaware that personally identifiable information will be collected about him or her in response to a request processed by the NAO.
2. Personally identifiable information may be collected, analyzed, or disseminated in a manner that makes the information inaccurate.
3. Personally identifiable information may be misused by a requestor.
4. Associated technology may improve so dramatically that qualitatively new capabilities will enable the gathering of personally identifiable information in ways that are impossible today, thus creating new potential privacy risks. (GAO, op. cit., p. 44)

DHS claims these issues will be mitigated by “providing appropriate oversight” and by “building a process to identify and correct inaccurate information, and ensuring that the DHS Privacy Office and DHS Office for Civil Rights and Civil Liberties remain critical components of all review processes as new and improved technology is developed.”

In other words, we’re to rely on DHS to police itself and that agencies critical to Office operations such as the National Reconnaissance Office and the National Geospatial-Intelligence Agency will simply hand over America’s most closely-guarded intelligence secrets to federal civil rights attorneys for appropriate “oversight.” Talk about a blind leap into the darkness!

Let’s be clear here and shed whatever illusions one may have about the outcome of last Tuesday’s election. Despite the overwhelming rejection of the Bush administration and their surrogates by the American people, the incoming Obama administration will pay lip-service to civil liberties and the rule of law. This however, will amount to no more than a better public relations campaign, image management and product roll-out. America rebranded.

But as we have seen throughout the unfolding disaster that is the “war on terror,” the Democrats have been fully complicit with the crimes of the Bush regime. From the USA Patriot Act, warrantless wiretapping, immunity for criminal telecoms, “preemptive policing,” torture, financial fraud and the looting of the economy by capitalist grifters, not to mention the invasion and occupation of Afghanistan and Iraq, threats against Russia, China, Iran, Pakistan, Bolivia, Cuba and Venezuela—indeed any nation that doesn’t toe the imperialist line—the Democrats have been Bush’s most faithful and reliable partners.

While the GAO’s report is a welcome addition to the already voluminous catalogue of Bushist horrors, one can expect that NAO’s law enforcement “mission” will quickly—and quietly—come on line. After all there’s bundles of cash, courtesy of the American people, that need to be spread far and wide!

**Tom Burghardt** is a researcher and activist based in the San Francisco Bay Area. In

addition to publishing in *Covert Action Quarterly* and [Global Research](#), an independent research and media group of writers, scholars, journalists and activists based in Montreal, his articles can be read on [Dissident Voice](#), [The Intelligence Daily](#) and [Pacific Free Press](#). He is the editor of *Police State America: U.S. Military "Civil Disturbance" Planning*, distributed by [AK Press](#).

The original source of this article is [Antifascist Calling](#)  
Copyright © [Tom Burghardt](#), [Antifascist Calling](#), 2008

---

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: **Tom Burghardt**  
<http://antifascist-calling.blogspot.com/>

**Disclaimer:** The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: [publications@globalresearch.ca](mailto:publications@globalresearch.ca)  
[www.globalresearch.ca](http://www.globalresearch.ca) contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: [publications@globalresearch.ca](mailto:publications@globalresearch.ca)