# National Security Agency

From Wikipedia, the free encyclopedia

*"NSA" redirects here. For other uses, see* [*NSA (disambiguation)*](http://en.wikipedia.org/wiki/NSA_%28disambiguation%29)*.*





|  |
| --- |
| **National Security Agency— NSA —** |
| Seal of the National Security Agency |
| Flag of the National Security Agency |
| **Agency overview** |
| **Formed** | November 4, 1952 (1952-11-04) |
| **Preceding Agency** | Armed Forces Security Agency |
| **Headquarters** | [Fort Meade](http://en.wikipedia.org/wiki/Fort_George_G._Meade), [Maryland](http://en.wikipedia.org/wiki/Maryland), U.S.[39°6′32″N 76°46′17″W﻿ / ﻿39.10889°N 76.77139°W﻿ / 39.10889; -76.77139](http://tools.wmflabs.org/geohack/geohack.php?pagename=National_Security_Agency&params=39_6_32_N_76_46_17_W_) |
| **Employees** | Classified (30,000-40,000 estimate)  |
| **Annual budget** | Classified ($10.8 billion, as of 2013)  |
| **Agency executives** | [General](http://en.wikipedia.org/wiki/General_%28United_States%29) [Keith B. Alexander](http://en.wikipedia.org/wiki/Keith_B._Alexander), [U.S. Army](http://en.wikipedia.org/wiki/United_States_Army), [Director of the National Security Agency](http://en.wikipedia.org/wiki/Director_of_the_National_Security_Agency)[John C. Inglis](http://en.wikipedia.org/wiki/John_C._Inglis), [Deputy Director of the National Security Agency](http://en.wikipedia.org/wiki/Deputy_Director_of_the_National_Security_Agency) |
| **Parent agency** | [United States Department of Defense](http://en.wikipedia.org/wiki/United_States_Department_of_Defense) |
| **Website** | [www.nsa.gov](http://www.nsa.gov) |

The **National Security Agency** (**NSA**) is the main producer and manager of [signals intelligence](http://en.wikipedia.org/wiki/Signals_intelligence) for the [United States](http://en.wikipedia.org/wiki/United_States). Estimated to be one of the largest of [U.S. intelligence organizations](http://en.wikipedia.org/wiki/US_intelligence_community#Organization) in terms of personnel and budget, the NSA operates under the jurisdiction of the [Department of Defense](http://en.wikipedia.org/wiki/United_States_Department_of_Defense) and reports to the [Director of National Intelligence](http://en.wikipedia.org/wiki/Director_of_National_Intelligence).

The NSA is tasked with the global monitoring, collection, [decoding](http://en.wikipedia.org/wiki/Codebreaking), translation and analysis of information and data for foreign intelligence and [counterintelligence](http://en.wikipedia.org/wiki/Counterintelligence) purposes, including surveillance of targeted individuals on U.S. soil. The agency is authorized to accomplish its mission through [clandestine means](http://en.wikipedia.org/wiki/Clandestine_operations), among which are [bugging](http://en.wikipedia.org/wiki/Bugging) electronic systems and allegedly engaging in [sabotage](http://en.wikipedia.org/wiki/Sabotage) through [subversive software](http://en.wikipedia.org/wiki/Stuxnet). The NSA is also responsible for the protection of U.S. government communications and information systems. As part of the growing practice of [mass surveillance in the United States](http://en.wikipedia.org/wiki/Mass_surveillance_in_the_United_States), the NSA collects and stores all phone records of all American citizens.

Unlike the [Defense Intelligence Agency](http://en.wikipedia.org/wiki/Defense_Intelligence_Agency) (DIA) and the [Central Intelligence Agency](http://en.wikipedia.org/wiki/Central_Intelligence_Agency) (CIA), both of which specialize primarily in foreign [human espionage](http://en.wikipedia.org/wiki/Clandestine_HUMINT), the NSA has no authority to conduct human-source intelligence gathering, although it is often [portrayed so](http://en.wikipedia.org/wiki/NSA_in_popular_culture) in [popular culture](http://en.wikipedia.org/wiki/Popular_culture). Instead, the NSA is entrusted with coordination and deconfliction of [SIGINT](http://en.wikipedia.org/wiki/SIGINT) components of otherwise non-SIGINT government organizations, which are prevented by law from engaging in such activities without the approval of the NSA via the Defense Secretary.

As part of these streamlining responsibilities, the agency has a co-located organization called the [Central Security Service](http://en.wikipedia.org/wiki/Central_Security_Service) (CSS), which was created to facilitate cooperation between NSA and other U.S. military cryptanalysis components. Additionally, the [NSA Director](http://en.wikipedia.org/wiki/Director_of_the_National_Security_Agency) simultaneously serves as the Commander of the [United States Cyber Command](http://en.wikipedia.org/wiki/United_States_Cyber_Command) and as Chief of the [Central Security Service](http://en.wikipedia.org/wiki/Central_Security_Service).

## History

The predecessor of the National Security Agency was the **Armed Forces Security Agency** (**AFSA**), created on May 20, 1949. This organization was originally established within the [U.S. Department of Defense](http://en.wikipedia.org/wiki/United_States_Department_of_Defense) under the command of the [Joint Chiefs of Staff](http://en.wikipedia.org/wiki/Joint_Chiefs_of_Staff). The AFSA was to direct Department of Defense communications and electronic intelligence activities, except those of U.S. [military intelligence](http://en.wikipedia.org/wiki/Military_intelligence) units. AFSA failed to achieve a centralized [communications intelligence](http://en.wikipedia.org/wiki/COMINT) mechanism, and failed to coordinate with civilian agencies that shared its interests (the [Department of State](http://en.wikipedia.org/wiki/United_States_Department_of_State), [CIA](http://en.wikipedia.org/wiki/Central_Intelligence_Agency), and [FBI](http://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation)).

In December 1951, President [Harry S. Truman](http://en.wikipedia.org/wiki/Harry_S._Truman) ordered a study to correct AFSA's failures. Six months later, the four members finished and issued the Brownell Report, which criticized AFSA, strengthened it and resulted in its redesignation as the National Security Agency. The agency was formally established by Truman in a memorandum of October 24, 1952, that revised [National Security Council Intelligence Directive (NSCID) 9](http://en.wikipedia.org/wiki/National_Security_Council_Intelligence_Directives). Truman's memo was later [declassified](http://en.wikipedia.org/wiki/Classified_information).

### Insignia



The [heraldic](http://en.wikipedia.org/wiki/Heraldic) insignia of NSA consists of an [eagle](http://en.wikipedia.org/wiki/Bald_eagle) inside a circle, grasping a [key](http://en.wikipedia.org/wiki/Key_%28lock%29) in its talons. The eagle represents the agency's national mission. Its breast features a shield with bands of red and white, taken from the [Great Seal of the United States](http://en.wikipedia.org/wiki/Great_Seal_of_the_United_States) and representing Congress. The key is taken from the emblem of [Saint Peter](http://en.wikipedia.org/wiki/Saint_Peter) and represents security.

When the NSA was created, the agency had no emblem and used that of the Department of Defense. The agency adopted its first of two emblems in 1963. The current NSA insignia has been in use since 1965, when then-[Director](http://en.wikipedia.org/wiki/Director_of_the_National_Security_Agency), LTG [Marshall S. Carter](http://en.wikipedia.org/wiki/Marshall_Carter) ([USA](http://en.wikipedia.org/wiki/United_States_Army)) ordered the creation of a device to represent the agency.

The NSA's flag consists of the agency's seal on a light blue background.

### Memorials





National Cryptologic Memorial

Crews associated with NSA missions have been involved in a number of dangerous and deadly situations. The [USS *Liberty* incident](http://en.wikipedia.org/wiki/USS_Liberty_incident) in 1967 and [USS *Pueblo* incident](http://en.wikipedia.org/wiki/USS_Pueblo_%28AGER-2%29) in 1968 are examples of the losses endured during the [Cold War](http://en.wikipedia.org/wiki/Cold_War).

The National Security Agency/Central Security Service Cryptologic Memorial honors and remembers the fallen personnel, both military and civilian, of these intelligence missions.[[22]](http://en.wikipedia.org/wiki/National_Security_Agency#cite_note-memorial-22#cite_note-memorial-22) It is made of black granite, and has 171 names (as of 2013) carved into it. It is located at NSA headquarters. A tradition of declassifying the stories of the fallen was begun in 2001.

In 1999, NSA founded the [NSA Hall of Honor](http://en.wikipedia.org/wiki/NSA_Hall_of_Honor), a memorial at the [National Cryptologic Museum](http://en.wikipedia.org/wiki/National_Cryptologic_Museum) in Fort Meade, Maryland. The memorial is a "tribute to the pioneers and heroes who have made significant and long-lasting contributions to American cryptology". NSA employees must be retired for more than fifteen years to qualify for the memorial.

### Mass surveillance disclosures

Main article: [2013 mass surveillance disclosures](http://en.wikipedia.org/wiki/2013_mass_surveillance_disclosures)

During the Watergate affair, as a result of A Congressional Inquiry led by Sen. Frank Church it was revealed that the NSA, in collaboration with Britain’s secret listening post, GCHQ, had routinely intercepted the international communications of prominent anti-Vietnam war leaders such as Jane Fonda and Dr. Benjamin Spock. A multi-year investigation by the European Parliament highlighted the NSA's role in economic espionage in a report entitled 'Development of Surveillance Technology and Risk of Abuse of Economic Information', in 1999. However it was a series of detailed disclosures of internal NSA documents in June 2013 that for the general public first revealed the massive extent of the NSA's spying, both foreign and domestic. Most of these were leaked by an ex-contractor, [Edward Snowden](http://en.wikipedia.org/wiki/Edward_Snowden). It was revealed that the NSA intercepts telephone and internet communications of over a billion people worldwide, seeking information on terrorism as well as foreign politics, economics and "commercial secrets". A [dedicated unit](http://en.wikipedia.org/w/index.php?title=Counter-Terrorism_Mission_Aligned_Cell&action=edit&redlink=1) of the NSA locates targets for the [CIA](http://en.wikipedia.org/wiki/CIA) for extrajudicial assassination in the Middle East. The NSA has also spied extensively on the European Union, the United Nations and numerous governments including allies and trading partners in Europe, South America and Asia.

The NSA reportedly has access to all communications made via Google, Microsoft, Facebook, Yahoo, YouTube, AOL, Skype, Apple and Paltalk, and collects hundreds of millions of contact lists from personal email and instant messaging accounts each year. It has also managed to weaken much of the encryption used on the Internet (by collaborating with, coercing or otherwise infiltrating numerous technology companies), so that the majority of Internet privacy is now vulnerable to the NSA and other attackers.

Domestically, the NSA collects metadata of the phone calls of over 120 million US [Verizon subscribers](http://en.wikipedia.org/wiki/MAINWAY) as well as internet communications, relying on a secret interpretation of the [Patriot Act](http://en.wikipedia.org/wiki/Patriot_Act) whereby the entirety of US communications may be considered "relevant" to a terrorism investigation if it is expected that even a tiny minority may relate to terrorism. The NSA supplies domestic intercepts to the [DEA](http://en.wikipedia.org/wiki/Drug_Enforcement_Administration), [IRS](http://en.wikipedia.org/wiki/Internal_Revenue_Service) and other law enforcement agencies, who use these to intitiate criminal investigations against US citizens. Federal agents are then instructed to "recreate" the investigative trail in order to "cover up" where the information originated.

Despite President Obama's claims that these programs have congressional oversight, members of Congress were unaware of the existence of these NSA programs or the secret interpretation of the Patriot Act, and have consistently been denied access to basic information about them. Obama has also claimed that there are legal checks in place to prevent inappropriate access of data and that there have been no examples of abuse; however, the secret FISC court charged with regulating the NSA's activities is, according to its chief judge, incapable of investigating or verifying how often the NSA breaks even its own secret rules. It has since been reported that the NSA violated its own rules on data access thousands of times a year, many of these violations involving large-scale data interceptions; and that NSA officers have even used data intercepts to spy on love interests. A March 2009 opinion of the FISC court, released by court order, states that protocols restricting data queries had been "so frequently and systemically violated that it can be fairly said that this critical element of the overall ... regime has never functioned effectively." Email contact lists (including those of US citizens) are collected at numerous foreign locations to work around the illegality of doing so on US soil.

Numerous conflicting stories have been put forward by the Obama administration in response to new revelations in the media. On March 20, 2013 the Director of National Intelligence, Admiral [James Clapper](http://en.wikipedia.org/wiki/James_Clapper) testified before Congress that the NSA doesn't wittingly collect any kind of data on millions or hundreds of millions of Americans, but he retracted this in June after details of the [PRISM](http://en.wikipedia.org/wiki/PRISM) program were published, and stated instead that meta-data of phone and internet traffic are collected, but no actual message contents. This was corroborated by NSA Director, General [Keith Alexander](http://en.wikipedia.org/wiki/Keith_B._Alexander), before it was revealed that the [XKeyscore](http://en.wikipedia.org/wiki/XKeyscore) program collects the contents of millions of emails from US citizens without warrant, as well as "nearly everything a user does on the Internet". Alexander later admitted that "content" is collected, but stated that it is simply stored and never analyzed or searched unless there is "a nexus to al-Qaida or other terrorist groups".

Regarding the necessity of these NSA programs, Gen. Alexander stated on June 27 that the NSA's bulk phone and Internet intercepts had been instrumental in preventing 54 terrorist "events", including 13 in the US, and in all but one of these cases had provided the initial tip to "unravel the threat stream". On July 31 NSA Deputy Director John Inglis conceded to the Senate that these intercepts had not been vital in stopping any terrorist attacks, but were "close" to vital in identifying and convicting four San Diego men for sending US$8,930 to [Al-Shabaab](http://en.wikipedia.org/wiki/Al-Shabaab_%28militant_group%29), a militia that conducts terrorism in Somalia.

The U.S. government has aggressively sought to dismiss and challenge [Fourth Amendment](http://en.wikipedia.org/wiki/Fourth_Amendment_to_the_United_States_Constitution) cases raised against it, and has granted retroactive immunity to ISPs and telecoms participating in domestic surveillance.

## Facilities

### Headquarters

Headquarters for the National Security Agency is located at

WikiMiniAtlas

[39°6′32″N 76°46′17″W﻿ / ﻿39.10889°N 76.77139°W﻿ / 39.10889; -76.77139](http://tools.wmflabs.org/geohack/geohack.php?pagename=National_Security_Agency&params=39_6_32_N_76_46_17_W_) in [Fort George G. Meade](http://en.wikipedia.org/wiki/Fort_George_G._Meade), [Maryland](http://en.wikipedia.org/wiki/Maryland), although it is separate from other compounds and agencies that are based within this same military installation. Ft. Meade is about 20 mi (32 km) southwest of [Baltimore](http://en.wikipedia.org/wiki/Baltimore), and 25 mi (40 km) northeast of Washington, DC. The NSA has its own exit off [Maryland Route 295 South](http://en.wikipedia.org/wiki/Baltimore%E2%80%93Washington_Parkway) labeled "NSA Employees Only". The exit may only be used by people with the proper clearances, and security vehicles parked along the road guard the entrance. NSA is the largest employer in the U.S. state of Maryland, and two-thirds of its personnel work at Ft. Meade. Built on 350 acres (140 ha; 0.55 sq mi) of Ft. Meade's 5,000 acres (2,000 ha; 7.8 sq mi), the site has 1,300 buildings and an estimated 18,000 parking spaces.

|  |  |  |
| --- | --- | --- |
|  |  |  |
| NSA headquarters building in [Fort Meade](http://en.wikipedia.org/wiki/Fort_George_G._Meade) (left), [NSOC](http://en.wikipedia.org/wiki/NSOC) (right) |

The main NSA headquarters and operations building is what [James Bamford](http://en.wikipedia.org/wiki/James_Bamford), author of [*Body of Secrets*](http://en.wikipedia.org/wiki/Body_of_Secrets), describes as "a modern boxy structure" that appears similar to "any stylish office building." The building is covered with one-way dark glass, which is lined with copper shielding in order to prevent espionage by trapping in signals and sounds. It contains 3,000,000 square feet (280,000 m2), or more than 68 acres (28 ha), of floor space; Bamford said that the [U.S. Capitol](http://en.wikipedia.org/wiki/U.S._Capitol) "could easily fit inside it four times over."

The facility has over 100 watchposts, one of them being the visitor control center, a two-story area that serves as the entrance. At the entrance, a white pentagonal structure, visitor badges are issued to visitors and security clearances of employees are checked. The visitor center includes a painting of the NSA seal. The OPS2A building, the tallest building in the NSA complex and the location of much of the agency's operations directorate, is accessible from the visitor center. Bamford described it as a "dark glass [Rubik's Cube](http://en.wikipedia.org/wiki/Rubik%27s_Cube)". The facility's "red corridor" houses non-security operations such as concessions and the drug store. The name refers to the "red badge" which is worn by someone without a security clearance. The NSA headquarters includes a cafeteria, a credit union, ticket counters for airlines and entertainment, a barbershop, and a bank. NSA headquarters has its own post office, fire department, and police force.

The employees at the NSA headquarters reside in various places in the [Baltimore-Washington area](http://en.wikipedia.org/wiki/Baltimore-Washington_area), including [Annapolis](http://en.wikipedia.org/wiki/Annapolis%2C_Maryland), Baltimore, and [Columbia](http://en.wikipedia.org/wiki/Columbia%2C_Maryland) in Maryland and the District of Columbia, including the [Georgetown](http://en.wikipedia.org/wiki/Georgetown%2C_District_of_Columbia) community.

#### Power consumption





Due to massive amounts of data processing, NSA is the largest electricity consumer in Maryland.

Following a major power outage in 2000, in 2003 and in follow-ups through 2007, [*The Baltimore Sun*](http://en.wikipedia.org/wiki/The_Baltimore_Sun) reported that the NSA was at risk of electrical overload because of insufficient internal electrical infrastructure at Fort Meade to support the amount of equipment being installed. This problem was apparently recognized in the 1990s but not made a priority, and "now the agency's ability to keep its operations going is threatened."

Baltimore Gas & Electric (BGE, now [Constellation Energy](http://en.wikipedia.org/wiki/Constellation_Energy)) provided NSA with 65 to 75 [megawatts](http://en.wikipedia.org/wiki/Kilowatt-hour#Watt_hour_multiples_and_billing_units) at Ft. Meade in 2007, and expected that an increase of 10 to 15 megawatts would be needed later that year. In 2011, NSA at Ft. Meade was Maryland's largest consumer of power. In 2007, as BGE's largest customer, NSA bought as much electricity as [Annapolis](http://en.wikipedia.org/wiki/Annapolis%2C_Maryland), the capital city of Maryland.

One estimate put the potential for power consumption by the new [Utah Data Center](http://en.wikipedia.org/wiki/Utah_Data_Center) at $40 million per year.

#### History of headquarters





Headquarters at Fort Meade circa 1950s

When the agency was established, its headquarters and cryptographic center were in the Naval Security Station in [Washington, D.C.](http://en.wikipedia.org/wiki/Washington%2C_D.C.). The COMINT functions were located in [Arlington Hall](http://en.wikipedia.org/wiki/Arlington_Hall) in [Northern Virginia](http://en.wikipedia.org/wiki/Northern_Virginia), which served as the headquarters of the [U.S. Army](http://en.wikipedia.org/wiki/United_States_Army)'s cryptographic operations. Because the [Soviet Union](http://en.wikipedia.org/wiki/Soviet_Union) had detonated a nuclear bomb and because the facilities were crowded, the federal government wanted to move several agencies, including the AFSA/NSA. A planning committee considered [Fort Knox](http://en.wikipedia.org/wiki/Fort_Knox), but [Fort Meade](http://en.wikipedia.org/wiki/Fort_George_G._Meade), [Maryland](http://en.wikipedia.org/wiki/Maryland), was ultimately chosen as NSA headquarters because it was far enough away from Washington, D.C. in case of a nuclear strike and was close enough so its employees would not have to move their families.

Construction of additional buildings began after the agency occupied buildings at Ft. Meade in the late 1950s, which they soon outgrew. In 1963 the new headquarters building, nine stories tall, opened. NSA workers referred to the building as the "Headquarters Building" and since the NSA management occupied the top floor, workers used "Ninth Floor" to refer to their leaders. COMSEC remained in Washington, D.C., until its new building was completed in 1968. In September 1986, the Operations 2A and 2B buildings, both copper-shielded to prevent [eavesdropping](http://en.wikipedia.org/wiki/Eavesdropping), opened with a dedication by President [Ronald Reagan](http://en.wikipedia.org/wiki/Ronald_Reagan). The four NSA buildings became known as the "Big Four." The NSA director moved to 2B when it opened.

#### Computing

In 1995, [*The Baltimore Sun*](http://en.wikipedia.org/wiki/The_Baltimore_Sun) reported that the NSA is the owner of the single largest group of [supercomputers](http://en.wikipedia.org/wiki/Supercomputer).

NSA held a groundbreaking ceremony at Ft. Meade in May 2013 for its High Performance Computing Center 2, expected to open in 2016. Called Site M, the center has a 150 megawatt power substation, 14 administrative buildings and 10 parking garages. It cost $3.2 billion and covers 227 acres (92 ha; 0.355 sq mi). The center is 1,800,000 square feet (17 ha; 0.065 sq mi) and initially uses 60 megawatts of electricity.

Increments II and III are expected to be completed by 2030, and would quadruple the space, covering 5,800,000 square feet (54 ha; 0.21 sq mi) with 60 buildings and 40 parking garages. [Defense contractors](http://en.wikipedia.org/wiki/Defense_contractor) are also establishing or expanding cybersecurity facilities near the NSA and around the [Washington metropolitan area](http://en.wikipedia.org/wiki/Washington_metropolitan_area).

### Other U.S. facilities





Buckley Air Force Base in Colorado

As of 2012, NSA collected intelligence from four [geostationary satellites](http://en.wikipedia.org/wiki/Geosynchronous_satellite). Satellite receivers were at Roaring Creek station in [Catawissa, Pennsylvania](http://en.wikipedia.org/wiki/Catawissa%2C_Pennsylvania) and Salt Creek in [Arbuckle, California](http://en.wikipedia.org/wiki/Arbuckle%2C_California). It operated ten to twenty [taps](http://en.wikipedia.org/wiki/Telephone_tapping) on U.S. telecom switches. NSA had installations in several U.S. states and from them observed intercepts from Europe, the Middle East, North Africa, Latin America, and Asia.

NSA had facilities at [Friendship Annex](http://en.wikipedia.org/wiki/Friendship_Annex) (FANX) in [Linthicum, Maryland](http://en.wikipedia.org/wiki/Linthicum%2C_Maryland), which is a 20 to 25-minute drive from Ft. Meade; the Aerospace Data Facility at [Buckley Air Force Base](http://en.wikipedia.org/wiki/Buckley_Air_Force_Base) in [Aurora](http://en.wikipedia.org/wiki/Aurora%2C_Colorado) outside [Denver](http://en.wikipedia.org/wiki/Denver), Colorado; NSA Texas in the [Texas Cryptology Center](http://en.wikipedia.org/wiki/Texas_Cryptology_Center) at [Lackland Air Force Base](http://en.wikipedia.org/wiki/Lackland_Air_Force_Base) in [San Antonio](http://en.wikipedia.org/wiki/San_Antonio), Texas; NSA Georgia at [Fort Gordon](http://en.wikipedia.org/wiki/Fort_Gordon) in [Augusta, Georgia](http://en.wikipedia.org/wiki/Augusta%2C_Georgia); NSA Hawaii in [Honolulu](http://en.wikipedia.org/wiki/Honolulu); the Multiprogram Research Facility in [Oak Ridge, Tennessee](http://en.wikipedia.org/wiki/Oak_Ridge%2C_Tennessee), and elsewhere.

On January 6, 2011 a groundbreaking ceremony was held to begin construction on NSA's first Comprehensive National Cyber-security Initiative (CNCI) Data Center, known as the "[Utah Data Center](http://en.wikipedia.org/wiki/Utah_Data_Center)" for short. The $1.5B data center is being built at [Camp Williams](http://en.wikipedia.org/wiki/Camp_Williams), [Utah](http://en.wikipedia.org/wiki/Utah), located 25 miles (40 km) south of [Salt Lake City](http://en.wikipedia.org/wiki/Salt_Lake_City), and will help support the agency's National Cyber-security Initiative. It is expected to be operational by September 2013.

In 2009, to protect its assets and to access more electricity, NSA sought to decentralize and expand its existing facilities in Ft. Meade and Menwith Hill, the latter expansion expected to be completed by 2015.

The [*Yakima Herald-Republic*](http://en.wikipedia.org/wiki/Yakima_Herald-Republic) cited Bamford, saying that many of NSA's bases for its Echelon program were a [legacy system](http://en.wikipedia.org/wiki/Legacy_system), using outdated, 1990s technology. In 2004, NSA closed its operations at [Bad Aibling Station](http://en.wikipedia.org/wiki/Bad_Aibling_Station) (Field Station 81) in [Bad Aibling](http://en.wikipedia.org/wiki/Bad_Aibling), Germany. In 2012, NSA began to move some of its operations at Yakima Research Station, [Yakima Training Center](http://en.wikipedia.org/wiki/Yakima_Training_Center), in Washington state to Colorado, planning to leave Yakima closed. As of 2013, NSA also intended to close operations at [Sugar Grove, West Virginia](http://en.wikipedia.org/wiki/Sugar_Grove%2C_West_Virginia).





[RAF Menwith Hill](http://en.wikipedia.org/wiki/RAF_Menwith_Hill) has the largest NSA presence in the United Kingdom.

### International stations

Following the signing in 1946–1956 of the [UKUSA Agreement](http://en.wikipedia.org/wiki/UKUSA_Agreement) between the United States, United Kingdom, Canada, Australia and New Zealand, who then cooperated on [signals intelligence](http://en.wikipedia.org/wiki/Signals_intelligence) and [Echelon](http://en.wikipedia.org/wiki/ECHELON), NSA stations were built at [GCHQ Bude](http://en.wikipedia.org/wiki/GCHQ_Bude) in [Morwenstow](http://en.wikipedia.org/wiki/Morwenstow), United Kingdom; [Geraldton](http://en.wikipedia.org/wiki/Geraldton), [Pine Gap](http://en.wikipedia.org/wiki/Pine_Gap) and Shoal Bay, Australia; [Leitrim](http://en.wikipedia.org/wiki/CFS_Leitrim) and [Ottawa](http://en.wikipedia.org/wiki/Ottawa), Canada; [Misawa](http://en.wikipedia.org/wiki/Misawa%2C_Aomori), Japan; and [Waihopai](http://en.wikipedia.org/wiki/Government_Communications_Security_Bureau#Waihopai_station) and [Tangimoana](http://en.wikipedia.org/wiki/Tangimoana), New Zealand.

NSA operates [RAF Menwith Hill](http://en.wikipedia.org/wiki/RAF_Menwith_Hill) in North Yorkshire, United Kingdom, which was, according to [BBC News](http://en.wikipedia.org/wiki/BBC_News) in 2007, the largest electronic monitoring station in the world. Planned in 1954, and opened in 1960, the base covered 562 acres (227 ha; 0.878 sq mi) as of 1999.

The agency's European Cryptologic Center (ECC), with 240 employees in 2011, is headquartered at a US military compound in [Griesheim](http://en.wikipedia.org/wiki/Griesheim_%28Hesse%29), near [Frankfurt](http://en.wikipedia.org/wiki/Frankfurt) in Germany. A 2011 NSA report indicates that the ECC is responsible for the "largest analysis and productivity in Europe" and focusses on various priorities, including Africa, Europe, the Middle East and counterterrorism operations.

In 2013, a new Consolidated Intelligence Center, also to be used by NSA, is being built at the headquarters of the [United States Army Europe](http://en.wikipedia.org/wiki/United_States_Army_Europe) in [Wiesbaden, Germany](http://en.wikipedia.org/wiki/Wiesbaden). NSA's partnership with [Bundesnachrichtendienst](http://en.wikipedia.org/wiki/Bundesnachrichtendienst) (BND), the German foreign intelligence service, was confirmed by BND president Gerhard Schindler.

## Organizational structure

The NSA is led by the [Director of the National Security Agency](http://en.wikipedia.org/wiki/Director_of_the_National_Security_Agency) (DIRNSA), who also serves as Chief of the [Central Security Service](http://en.wikipedia.org/wiki/Central_Security_Service) (CHCSS) and Commander of the [United States Cyber Command](http://en.wikipedia.org/wiki/United_States_Cyber_Command) (USCYBERCOM) and is the highest-ranking military official of these organizations. He is assisted by a [Deputy Director](http://en.wikipedia.org/wiki/Deputy_Director_of_the_National_Security_Agency), who is the highest-ranking civilian within the NSA/CSS.

NSA also has an [Inspector General](http://en.wikipedia.org/wiki/Inspector_General), head of the Office of the Inspector General (OIG), a [General Counsel](http://en.wikipedia.org/wiki/General_Counsel), head of the Office of the General Counsel (OGC) and a Director of Compliance, who is head of the Office of the Director of Compliance (ODOC).

Unlike other intelligence organizations such as CIA or [DIA](http://en.wikipedia.org/wiki/Defense_Intelligence_Agency), NSA has always been particularly reticent concerning its internal organizational structure.

As of the mid-1990s, the National Security Agency was organized into five Directorates:

* The Operations Directorate, which was responsible for SIGINT collection and processing.
* The Technology and Systems Directorate, which develops new technologies for SIGINT collection and processing.
* The Information Systems Security Directorate, which was responsible for NSA's communications and information security missions.
* The Plans, Policy and Programs Directorate, which provided staff support and general direction for the Agency.
* The Support Services Directorate, which provided logistical and administrative support activities.

Each of these directorates consisted of several groups or elements, designated by a letter. There were for example the A Group, which was responsible for all SIGINT operations against the Soviet Union and Eastern Europe, and G Group, which was responsible for SIGINT related to all non-communist countries. These groups were divided in units designated by an additional number, like unit A5 for breaking Soviet codes, and G6, being the office for the Middle East, North Africa, Cuba, Central and South America.

### Current structure

Currently, NSA has about a dozen directorates, which are designated by a letter, although not all of them are known. The directorates are divided in divisions and units, which have a designation which starts with the letter of the parent directorate, followed by a number for the division, the sub-unit or a sub-sub-unit. New information about NSA units was revealed in top secret documents leaked by [Edward Snowden](http://en.wikipedia.org/wiki/Edward_Snowden) since June 2013.

The main elements of the current organizational structure of the NSA are:

* F - Directorate only known from unit F6, the [**Special Collection Service**](http://en.wikipedia.org/wiki/Special_Collection_Service) (SCS), which is a joint program created by CIA and NSA in 1978 to facilitate clandestine activities such as [bugging](http://en.wikipedia.org/wiki/Bugging) computers throughout the world, using the expertise of both agencies.
* G - Directorate only known from unit G112, the office that manages the [Senior Span](http://en.wikipedia.org/wiki/Senior_Span) platform, attached to the U2 spy planes.
* **I - Information Assurance Directorate (IAD)**, which ensures the availability, integrity, authentication, confidentiality, and non-repudiation of national security and telecommunications and information systems (national security systems).
* J - Directorate only known from unit J2, the Cryptologic Intelligence Unit
* **L - Installation and Logistics**
* **M - Human Resources**
* **Q - Security and Counterintelligence**
* **R - Research Directorate**, which conducts research on signals intelligence and on information assurance for the U.S. Government.
* **S - Signals Intelligence Directorate (SID)**, which is responsible for the collection, analysis, production and dissemination of signals intelligence. This directorate is led by a director and a deputy director. The SID consists of the following divisions:
	+ **S1 - Customer Relations**
	+ **S2 - Analysis and Production Centers**, with the following so-called Product Lines:
		- S2A: South Asia, S2B: China and Korea, S2C: International Security, S2E: Middle East/Asia, S2F: International Crime, S2G: Counter-proliferation, S2H: Russia, S2I: Counter-terrorism, S2J: Weapons and Space, S2T: Current Threats
	+ **S3 - Data Acquisition**, with these divisions for the main collection programs:
		- **S31 - Cryptanalysis and Exploitation Services (CES)**
		- **S32 -** [**Tailored Access Operations**](http://en.wikipedia.org/wiki/Office_of_Tailored_Access_Operations) **(TAO)**, which hacks into foreign computers to conduct cyber-espionage and reportedly is "the largest and arguably the most important component of the NSA's huge Signal Intelligence (SIGINT) Directorate, consisting of over 1,000 military and civilian computer hackers, intelligence analysts, targeting specialists, computer hardware and software designers, and electrical engineers."
		- **S33 - Global Access Operations (GAO)**, which is responsible for intercepts from satellites and other international SIGINT platforms. A tool which details and maps the information collected by this unit is code-named [Boundless Informant](http://en.wikipedia.org/wiki/Boundless_Informant).
		- **S34 - Collections Strategies and Requirements Center**
		- **S35 -** [**Special Source Operations**](http://en.wikipedia.org/wiki/Special_Source_Operations) **(SSO)**, which is responsible for domestic and compartmented collection programs, like for example the [PRISM](http://en.wikipedia.org/wiki/PRISM) program.[[104]](http://en.wikipedia.org/wiki/National_Security_Agency#cite_note-theweek.com-104#cite_note-theweek.com-104) Special Source Operations is also mentioned in connection to the [FAIRVIEW](http://en.wikipedia.org/wiki/Fairview_%28surveillance_program%29) collection program.
* **T - Technical Directorate (TD)**
* **Directorate for Education and Training**
* **Directorate for Corporate Leadership**
* **Foreign Affairs Directorate**, which acts as liaison with foreign intelligence services, counter-intelligence centers and the UKUSA-partners.
* **Acquisitions and Procurement Directorate**

In the year 2000, a leadership team was formed, consisting of the Director, the Deputy Director and the Directors of the Signals Intelligence (SID), the Information Assurance (IAD) and the Technical Directorate (TD). The chiefs of other main NSA divisions became associate directors of the senior leadership team.

After president George W. Bush initiated the [President's Surveillance Program](http://en.wikipedia.org/wiki/President%27s_Surveillance_Program) (PSP) in 2001, the NSA created a 24-hour Metadata Analysis Center (MAC), followed in 2004 by the Advanced Analysis Division (AAD), which had to analyze content, internet metadata and telephone metadata. Both units were part of the Signals Intelligence Directorate.

There's also an office of Information Sharing Services (ISS), lead by a chief and a deputy chief

### Watch centers

The NSA maintains at least two watch centers:

* [**National Security Operations Center (NSOC)**](http://en.wikipedia.org/wiki/National_Security_Operations_Center), which is the NSA's current operations center and focal point for time-sensitive SIGINT reporting for the United States SIGINT System (USSS). This center was established in 1968 as the National SIGINT Watch Center (NSWC) and renamed into National SIGINT Operations Center (NSOC) in 1973. This "nerve center of the NSA" got its current name in 1996.
* **NSA/CSS Threat Operations Center (NTOC)**, which is the primary NSA/CSS partner for [Department of Homeland Security](http://en.wikipedia.org/wiki/Department_of_Homeland_Security) response to cyber incidents. The NTOC establishes real-time network awareness and threat characterization capabilities to forecast, alert, and attribute malicious activity and enable the coordination of Computer Network Operations. The NTOC was established in 2004 as a joint Information Assurance and Signals Intelligence project.

### Employees

The number of NSA employees is officially classified but there are a number of sources providing estimates. In 1961, NSA had 59,000 military and civilian employees, which grew to 93,067 in 1969, of which 19,300 worked at the headquarters at Fort Meade. In the early 1980s NSA had roughly 50,000 military and civilian personnel. By 1989 this number had grown again to 75,000, of which 25,000 worked at the NSA headquarters. Between 1990 and 1995 the NSA's budget and workforce were cut by one third, which led to a substantial loss of experience.

In 2012, the NSA said more than 30,000 employees work at Ft. Meade and other facilities. In 2012 [John C. Inglis](http://en.wikipedia.org/wiki/John_C._Inglis), the deputy director, said that the total number of NSA employees is "somewhere between 37,000 and one billion" as a joke, and stated that the agency is "probably the biggest employer of [introverts](http://en.wikipedia.org/wiki/Introvert)." In 2013 [*Der Spiegel*](http://en.wikipedia.org/wiki/Der_Spiegel) stated that the NSA had 40,000 employees. More widely, it has been described as the world's largest single employer of [mathematicians](http://en.wikipedia.org/wiki/Mathematicians). Some NSA employees form part of the workforce of the [National Reconnaissance Office](http://en.wikipedia.org/wiki/National_Reconnaissance_Office) (NRO), the agency that provides the NSA with satellite [signals intelligence](http://en.wikipedia.org/wiki/Signals_intelligence).

As of 2013 about 1,000 [system administrators](http://en.wikipedia.org/wiki/System_administrator) work for the NSA.[[113]](http://en.wikipedia.org/wiki/National_Security_Agency#cite_note-DrewSengupta-113#cite_note-DrewSengupta-113) [Edward Snowden](http://en.wikipedia.org/wiki/Edward_Snowden)'s leaking of [PRISM](http://en.wikipedia.org/wiki/PRISM) in 2013 caused the NSA to institute a "[two-man rule](http://en.wikipedia.org/wiki/Two-man_rule)" where two system administrators are required to be present when one accesses certain sensitive information.

#### Polygraphing





NSA polygraph brochure

The NSA conducts [polygraph](http://en.wikipedia.org/wiki/Polygraph) tests of employees. For new employees, the tests are meant to discover enemy spies who are applying to the NSA and to uncover any information that could make an applicant pliant to coercion. As part of the latter, historically *EPQs* or "embarrassing personal questions" about sexual behavior had been included in the NSA polygraph. The NSA also conducts five-year periodic reinvestigation polygraphs of employees, focusing on counterintelligence programs. In addition the NSA conducts aperiodic polygraph investigations in order to find spies and leakers; those who refuse to take them may receive "termination of employment", according to a 1982 memorandum from the director of the NSA.





NSA-produced video on the polygraph process

There are also "special access examination" polygraphs for employees who wish to work in highly sensitive areas, and those polygraphs cover counterintelligence questions and some questions about behavior. NSA's brochure states that the average test length is between two and four hours. A 1983 report of the [Office of Technology Assessment](http://en.wikipedia.org/wiki/Office_of_Technology_Assessment) stated that "It appears that the NSA [National Security Agency] (and possibly CIA) use the polygraph not to determine deception or truthfulness per se, but as a technique of interrogation to encourage admissions." Sometimes applicants in the polygraph process confess to committing felonies such as murder, rape, and selling of illegal drugs. Between 1974 and 1979, of the 20,511 job applicants who took polygraph tests, 695 (3.4%) confessed to previous felony crimes; almost all of those crimes had been undetected.

In 2010 the NSA produced a video explaining its polygraph process. The video, ten minutes long, is titled "The Truth About the Polygraph" and was posted to the website of the [Defense Security Service](http://en.wikipedia.org/wiki/Defense_Security_Service). Jeff Stein of [*The Washington Post*](http://en.wikipedia.org/wiki/The_Washington_Post) said that the video portrays "various applicants, or actors playing them -- it’s not clear -- describing everything bad they had heard about the test, the implication being that none of it is true." AntiPolygraph.org argues that the NSA-produced video omits some information about the polygraph process; it produced a video responding to the NSA video. George Maschke, the founder of the website, accused the NSA polygraph video of being "[Orwellian](http://en.wikipedia.org/wiki/Orwellian)".

## Operations

### Mission

NSA's [eavesdropping](http://en.wikipedia.org/wiki/Eavesdropping) mission includes radio broadcasting, both from various organizations and individuals, the Internet, telephone calls, and other intercepted forms of communication. Its secure communications mission includes military, diplomatic, and all other sensitive, confidential or secret government communications.

According to the [*Washington Post*](http://en.wikipedia.org/wiki/Washington_Post), "[e]very day, collection systems at the National Security Agency intercept and store 1.7 billion e-mails, phone calls and other types of communications. The NSA sorts a fraction of those into 70 separate databases."

Because of its listening task, NSA/CSS has been heavily involved in [cryptanalytic](http://en.wikipedia.org/wiki/Cryptanalysis) research, continuing the work of predecessor agencies which had broken many World War II [codes](http://en.wikipedia.org/wiki/Code_%28cryptography%29) and [ciphers](http://en.wikipedia.org/wiki/Cipher) (see, for instance, [Purple](http://en.wikipedia.org/wiki/Purple_%28cipher_machine%29), [Venona project](http://en.wikipedia.org/wiki/Venona_project), and [JN-25](http://en.wikipedia.org/wiki/JN-25)).

In 2004, NSA [Central Security Service](http://en.wikipedia.org/wiki/Central_Security_Service) and the [National Cyber Security Division](http://en.wikipedia.org/wiki/National_Cyber_Security_Division) of the [Department of Homeland Security](http://en.wikipedia.org/wiki/Department_of_Homeland_Security) (DHS) agreed to expand NSA Centers of Academic Excellence in Information Assurance Education Program.

As part of the National Security [Presidential Directive](http://en.wikipedia.org/wiki/Presidential_Directive) 54/Homeland Security Presidential Directive 23 (NSPD 54), signed on January 8, 2008 by President Bush, the NSA became the lead agency to monitor and protect all of the federal government's computer networks from [cyber-terrorism](http://en.wikipedia.org/wiki/Cyber-terrorism).

### Echelon

Main article: [ECHELON](http://en.wikipedia.org/wiki/ECHELON)

Echelon was created in the incubator of the [Cold War](http://en.wikipedia.org/wiki/Cold_War). Today it is a [legacy system](http://en.wikipedia.org/wiki/Legacy_system), and several NSA stations are closing.

NSA/CSS, in combination with the equivalent agencies in the United Kingdom ([Government Communications Headquarters](http://en.wikipedia.org/wiki/Government_Communications_Headquarters)), Canada ([Communications Security Establishment](http://en.wikipedia.org/wiki/Communications_Security_Establishment)), Australia ([Defence Signals Directorate](http://en.wikipedia.org/wiki/Defence_Signals_Directorate)), and New Zealand ([Government Communications Security Bureau](http://en.wikipedia.org/wiki/Government_Communications_Security_Bureau)), otherwise known as the [UKUSA](http://en.wikipedia.org/wiki/UKUSA_Agreement) group, was reported to be in command of the operation of the so-called [Echelon](http://en.wikipedia.org/wiki/ECHELON) system. Its capabilities were suspected to include the ability to monitor a large proportion of the world's transmitted civilian telephone, fax and data traffic.

During the early 1970s, the first of what became more than eight large satellite communications dishes were installed at Menwith Hill. Investigative journalist [Duncan Campbell](http://en.wikipedia.org/wiki/Duncan_Campbell_%28journalist%29) reported in 1988 on the [Echelon](http://en.wikipedia.org/wiki/ECHELON) surveillance program, an extension of the [UKUSA Agreement](http://en.wikipedia.org/wiki/UKUSA_Agreement) on global signals intelligence [SIGINT](http://en.wikipedia.org/wiki/SIGINT), and detailed how the eavesdropping operations worked. In November 3, 1999 the BBC reported that they had confirmation from the Australian Government of the existence of a powerful "global spying network" code-named Echelon, that could "eavesdrop on every single phone call, fax or e-mail, anywhere on the planet" with Britain and the United States as the chief protagonists. They confirmed that Menwith Hill was "linked directly to the headquarters of the US National Security Agency (NSA) at Fort Meade in Maryland".

NSA's United States Signals Intelligence Directive 18 (USSID 18) strictly prohibited the interception or collection of information about "... U.S. persons, entities, corporations or organizations...." without explicit written legal permission from the [United States Attorney General](http://en.wikipedia.org/wiki/United_States_Attorney_General) when the subject is located abroad, or the [Foreign Intelligence Surveillance Court](http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Court) when within U.S. borders. Alleged Echelon-related activities, including its use for motives other than national security, including political and [industrial espionage](http://en.wikipedia.org/wiki/Industrial_espionage), received criticism from countries outside the UKUSA alliance.

### Data mining





Protesters against NSA data mining in [Berlin](http://en.wikipedia.org/wiki/Berlin) wearing [Bradley Manning](http://en.wikipedia.org/wiki/Bradley_Manning) and [Edward Snowden](http://en.wikipedia.org/wiki/Edward_Snowden) masks.

Main articles: [PRISM (surveillance program)](http://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29), [Data mining](http://en.wikipedia.org/wiki/Data_mining), [analytics](http://en.wikipedia.org/wiki/Analytics), [information extraction](http://en.wikipedia.org/wiki/Information_extraction), and [data analysis](http://en.wikipedia.org/wiki/Data_analysis)

NSA is reported to use its computing capability to analyze "transactional" data that it regularly acquires from other government agencies, which gather it under their own jurisdictional authorities. As part of this effort, NSA now monitors huge volumes of records of domestic emails and Internet searches as well as bank transfers, credit-card transactions and travel and telephone records, according to current and former intelligence officials interviewed by [*The Wall Street Journal*](http://en.wikipedia.org/wiki/The_Wall_Street_Journal). Reportedly, the majority of emails in or out of the USA are captured at "selected communications links" and automatically analyzed for keywords or other "selectors".

The NSA began the [PRISM](http://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29) electronic surveillance and [data mining](http://en.wikipedia.org/wiki/Data_mining) program in 2007.[[133]](http://en.wikipedia.org/wiki/National_Security_Agency#cite_note-WaPo1-133#cite_note-WaPo1-133)[[134]](http://en.wikipedia.org/wiki/National_Security_Agency#cite_note-Greenwald1-134#cite_note-Greenwald1-134) [PRISM](http://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29) gathers communications data on foreign targets from nine major U.S. internet-based communication service providers: [Microsoft](http://en.wikipedia.org/wiki/Microsoft), [Yahoo](http://en.wikipedia.org/wiki/Yahoo), [Google](http://en.wikipedia.org/wiki/Google), [Facebook](http://en.wikipedia.org/wiki/Facebook), [PalTalk](http://en.wikipedia.org/wiki/PalTalk), [AOL](http://en.wikipedia.org/wiki/AOL), [Skype](http://en.wikipedia.org/wiki/Skype), [YouTube](http://en.wikipedia.org/wiki/YouTube) and [Apple](http://en.wikipedia.org/wiki/Apple_Inc). Data gathered include email, video and voice chat, videos, photos, [VoIP](http://en.wikipedia.org/wiki/VoIP) chats such as Skype, and file transfers. Another program, [Boundless Informant](http://en.wikipedia.org/wiki/Boundless_Informant), employs [big data](http://en.wikipedia.org/wiki/Big_data) databases, [cloud computing](http://en.wikipedia.org/wiki/Cloud_computing) technology, and [Free and Open Source Software](http://en.wikipedia.org/wiki/Free_and_Open_Source_Software) (FOSS) to analyze data collected worldwide by the NSA, including that gathered by way of the [PRISM](http://en.wikipedia.org/wiki/PRISM_%28surveillance_program%29) program.

The Real Time Regional Gateway was a data collection program introduced in 2005 in Iraq by NSA during the [Iraq War](http://en.wikipedia.org/wiki/Iraq_War). It consisted of gathering all Iraqi electronic communication, storing it, then searching and otherwise analyzing it. It was effective in providing information about Iraqi insurgents who had eluded less comprehensive techniques. [Glenn Greenwald](http://en.wikipedia.org/wiki/Glenn_Greenwald) of [*The Guardian*](http://en.wikipedia.org/wiki/The_Guardian) believes that the "collect it all" strategy introduced by NSA director Alexander shows that "the NSA's goal is to collect, monitor and store every telephone and internet communication" worldwide.

### Encryption

In 2013, reporters uncovered a secret memo that claims the NSA created and pushed for the adoption of encryption standards that contained built-in vulnerabilities in 2006 to the United States [National Institute of Standards and Technology](http://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) (NIST), and the [International Organization for Standardization](http://en.wikipedia.org/wiki/International_Organization_for_Standardization) (aka ISO). This memo appears to give credence to previous speculation by cryptographers at Microsoft Research.

[Edward Snowden](http://en.wikipedia.org/wiki/Edward_Snowden) claims that the NSA often bypasses encryption altogether by lifting information before it is encrypted or after it is decrypted.

## Domestic activity

*Further information:* [*USA surveillance tools*](http://en.wikipedia.org/w/index.php?title=USA_surveillance_tools&action=edit&redlink=1) *and* [*Mass surveillance in the United States*](http://en.wikipedia.org/wiki/Mass_surveillance_in_the_United_States)

NSA's mission, as set forth in [Executive Order 12333](http://en.wikipedia.org/wiki/Executive_Order_12333), is to collect information that constitutes "foreign intelligence or counterintelligence" while *not* "acquiring information concerning the domestic activities of United States persons". NSA has declared that it relies on the FBI to collect information on foreign intelligence activities within the borders of the USA, while confining its own activities within the USA to the embassies and missions of foreign nations.

NSA's domestic surveillance activities are limited by the requirements imposed by the [Fourth Amendment to the U.S. Constitution](http://en.wikipedia.org/wiki/Fourth_Amendment_to_the_U.S._Constitution). The [Foreign Intelligence Surveillance Court](http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Court) for example held in October 2011, citing multiple Supreme Court precedents, that the Fourth Amendment prohibitions against unreasonable searches and seizures applies to the contents of all communications, whatever the means, because "a person's private communications are akin to personal papers." However, these protections do not apply to non-U.S. persons located outside of U.S. borders, so the NSA's foreign surveillance efforts are subject to far fewer limitations under U.S. law. The specific requirements for domestic surveillance operations are contained in the [Foreign Intelligence Surveillance Act](http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act) of 1978 (FISA), which does not extend protection to non-U.S. citizens located outside of [U.S. territory](http://en.wikipedia.org/wiki/U.S._territory).

These activities, especially the publicly acknowledged domestic telephone tapping and call database programs, have prompted questions about the extent of the NSA's activities and concerns about threats to privacy and the [rule of law](http://en.wikipedia.org/wiki/Rule_of_law).

In August 2013 it was revealed that NSA intelligence intercepts and wiretaps, both foreign and domestic, were being supplied to the [Drug Enforcement Administration](http://en.wikipedia.org/wiki/Drug_Enforcement_Administration) (DEA) and [Internal Revenue Service](http://en.wikipedia.org/wiki/Internal_Revenue_Service) (IRS) and were illegally used to launch criminal investigations of US citizens. Law enforcement agents were directed to conceal how the investigations began and recreate an apparently legal investigative trail by re-obtaining the same evidence by other means.

### Criticism

The NSA received criticism early on in 1960 after two agents had defected to the [Soviet Union](http://en.wikipedia.org/wiki/Soviet_Union). Investigations by the [House Un-American Activities Committee](http://en.wikipedia.org/wiki/House_Un-American_Activities_Committee) and a special subcommittee of the [House Armed Services Committee](http://en.wikipedia.org/wiki/House_Armed_Services_Committee) revealed severe cases of ignorance in personnel security regulations, prompting the former personnel director and the director of security to step down and leading to the adoption of stricter security practices. Nonetheless, security breaches reoccurred only a year later when in an issue of [*Izvestia*](http://en.wikipedia.org/wiki/Izvestia) of July 23, 1963, a former NSA employee published several cryptologic secrets. The very same day, an NSA clerk-messenger committed suicide as ongoing investigations disclosed that he had sold secret information to the Soviets on a regular basis. The reluctance of Congressional houses to look into these affairs had prompted a journalist to write "If a similar series of tragic blunders occurred in any ordinary agency of Government an aroused public would insist that those responsible be officially censured, demoted, or fired." [David Kahn](http://en.wikipedia.org/wiki/David_Kahn_%28writer%29) criticized the NSA's tactics of concealing its doings as smug and the Congress' blind faith in the agency's right-doing as shortsighted, and pointed out the necessity of surveillance by the Congress to prevent abuse of power.

The number of exemptions from legal requirements has also been criticized. When in 1964 the Congress was hearing a bill giving the director of the NSA the power to fire at will any employee, the Washington Post wrote: "This is the very definition of arbitrariness. It means that an employee could be discharged and disgraced on the basis of anonymous allegations without the slightest opportunity to defend himself." Yet, the bill was accepted by an overwhelming majority.

Polls conducted in June 2013 found divided results among Americans regarding NSA's secret data collection. [Rasmussen Reports](http://en.wikipedia.org/wiki/Rasmussen_Reports) found that 59% of Americans disapprove, [Gallup](http://en.wikipedia.org/wiki/Gallup_%28company%29) found that 53% disapprove and [Pew](http://en.wikipedia.org/wiki/Pew_Research_Center) found that 56% are in favor of NSA data collection.

### NSA monitoring under President Johnson

Main article: [Project MINARET](http://en.wikipedia.org/wiki/Project_MINARET)

In a secret 1960s operation code-named "Minaret", the NSA monitored phone communications of Senators [Frank Church](http://en.wikipedia.org/wiki/Frank_Church) and [Howard Baker](http://en.wikipedia.org/wiki/Howard_Baker), major civil rights leaders, including [Dr. Martin Luther King](http://en.wikipedia.org/wiki/Dr._Martin_Luther_King), and prominent U.S. journalists and athletes who criticized the U.S. war in Vietnam. A review by NSA of the NSA's Minaret program concluded that Minaret was "disreputable if not outright illegal."

### Domestic wiretapping under Richard Nixon

Further information: [Church Committee](http://en.wikipedia.org/wiki/Church_Committee)

In the years after President [Richard Nixon](http://en.wikipedia.org/wiki/Richard_Nixon) resigned, there were several investigations of suspected misuse of [Federal Bureau of Investigation](http://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation) (FBI), [Central Intelligence Agency](http://en.wikipedia.org/wiki/Central_Intelligence_Agency) (CIA), and NSA facilities. Senator [Frank Church](http://en.wikipedia.org/wiki/Frank_Church) headed a Senate investigating committee (the [Church Committee](http://en.wikipedia.org/wiki/Church_Committee)) which uncovered previously unknown activity, such as a CIA plot (ordered by the administration of President [John F. Kennedy](http://en.wikipedia.org/wiki/John_F._Kennedy)) to assassinate [Fidel Castro](http://en.wikipedia.org/wiki/Fidel_Castro). The investigation also uncovered NSA's wiretaps on targeted American citizens. After the Church Committee hearings, the [Foreign Intelligence Surveillance Act](http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act) of 1978 became law, limiting circumstances under which domestic surveillance was allowed.

### IT projects: ThinThread, Trailblazer, Turbulence

NSA created new IT systems to deal with the flood of information from new technologies like the internet and cellphones.

[ThinThread](http://en.wikipedia.org/wiki/ThinThread) contained advanced [data mining](http://en.wikipedia.org/wiki/Data_mining) capabilities. It also had a 'privacy mechanism'; surveillance was stored encrypted; decryption required a warrant. The research done under this program may have contributed to the technology used in later systems. ThinThread was cancelled when [Michael Hayden](http://en.wikipedia.org/wiki/Michael_Hayden_%28general%29) chose [Trailblazer](http://en.wikipedia.org/wiki/Trailblazer_Project), which did not include ThinThread's privacy system.

[Trailblazer Project](http://en.wikipedia.org/wiki/Trailblazer_Project) ramped up circa 2000. [SAIC](http://en.wikipedia.org/wiki/Science_Applications_International_Corporation), [Boeing](http://en.wikipedia.org/wiki/Boeing), [CSC](http://en.wikipedia.org/wiki/Computer_Sciences_Corporation), [IBM](http://en.wikipedia.org/wiki/IBM), and [Litton](http://en.wikipedia.org/wiki/Litton_Industries) worked on it. Some NSA [whistleblowers](http://en.wikipedia.org/wiki/Whistleblower) complained internally about major problems surrounding Trailblazer. This led to investigations by Congress and the NSA and DoD [Inspectors General](http://en.wikipedia.org/wiki/Inspectors_General). The project was cancelled circa 2003-4; it was late, over budget, and didn't do what it was supposed to do. The Baltimore Sun ran articles about this in 2006–07. The government then raided the whistleblowers' houses. One of them, [Thomas Drake](http://en.wikipedia.org/wiki/Thomas_Andrews_Drake), was charged with violating [18 U.S.C.](http://en.wikipedia.org/wiki/Title_18_of_the_United_States_Code) [§ 793(e)](http://www.law.cornell.edu/uscode/18/793.html#e) in 2010 in an unusual use of [espionage law](http://en.wikipedia.org/wiki/Espionage_Act). He and his defenders claim that he was actually being persecuted for challenging the Trailblazer Project. In 2011, all 10 original charges against Drake were dropped.

[Turbulence](http://en.wikipedia.org/wiki/Turbulence_%28NSA%29) started circa 2005. It was developed in small, inexpensive 'test' pieces rather than one grand plan like Trailblazer. It also included offensive cyber-warfare capabilities, like injecting [malware](http://en.wikipedia.org/wiki/Malware) into remote computers. Congress criticized Turbulence in 2007 for having similar bureaucratic problems as Trailblazer. It was to be a realization of information processing at higher speeds in cyberspace.

### Warrantless wiretaps under George W. Bush

Main article: [NSA warrantless surveillance (2001–07)](http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_%282001%E2%80%9307%29)

On December 16, 2005, [*The New York Times*](http://en.wikipedia.org/wiki/The_New_York_Times) reported that, under [White House](http://en.wikipedia.org/wiki/White_House) pressure and with an [executive order](http://en.wikipedia.org/wiki/Executive_order) from President [George W. Bush](http://en.wikipedia.org/wiki/George_W._Bush), the National Security Agency, in an attempt to thwart terrorism, had been tapping phone calls made to persons outside the country, without obtaining [warrants](http://en.wikipedia.org/wiki/Warrant_%28law%29) from the [United States Foreign Intelligence Surveillance Court](http://en.wikipedia.org/wiki/United_States_Foreign_Intelligence_Surveillance_Court), a secret court created for that purpose under the [Foreign Intelligence Surveillance Act](http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act) (FISA).

One such surveillance program, authorized by the U.S. Signals Intelligence Directive 18 of President George Bush, was the Highlander Project undertaken for the National Security Agency by the U.S. Army 513th Military Intelligence Brigade. NSA relayed telephone (including cell phone) conversations obtained from ground, airborne, and satellite monitoring stations to various U.S. Army Signal Intelligence Officers, including the 201st Military Intelligence Battalion. Conversations of citizens of the U.S. were intercepted, along with those of other nations.

Proponents of the surveillance program claim that the President has [executive authority](http://en.wikipedia.org/wiki/Unitary_executive_theory) to order such action, arguing that laws such as FISA are overridden by the President's Constitutional powers. In addition, some argued that FISA was implicitly overridden by a subsequent statute, the [Authorization for Use of Military Force](http://en.wikipedia.org/wiki/Authorization_for_Use_of_Military_Force_Against_Terrorists), although the Supreme Court's ruling in [Hamdan v. Rumsfeld](http://en.wikipedia.org/wiki/Hamdan_v._Rumsfeld) deprecates this view. In the August 2006 case [*ACLU v. NSA*](http://en.wikipedia.org/wiki/ACLU_v._NSA), [U.S. District Court](http://en.wikipedia.org/wiki/U.S._District_Court) Judge [Anna Diggs Taylor](http://en.wikipedia.org/wiki/Anna_Diggs_Taylor) concluded that NSA's warrantless surveillance program was both illegal and unconstitutional. On July 6, 2007 the [6th Circuit Court of Appeals](http://en.wikipedia.org/wiki/6th_Circuit_Court_of_Appeals) vacated the decision on the grounds that the ACLU lacked standing to bring the suit.

On January 17, 2006, the [Center for Constitutional Rights](http://en.wikipedia.org/wiki/Center_for_Constitutional_Rights) filed a lawsuit, [CCR v. Bush](http://en.wikipedia.org/wiki/CCR_v._Bush), against the [George W. Bush](http://en.wikipedia.org/wiki/George_W._Bush) Presidency. The lawsuit challenged the National Security Agency's (NSA's) surveillance of people within the U.S., including the interception of CCR emails without securing a warrant first.

In September 2008, the [Electronic Frontier Foundation](http://en.wikipedia.org/wiki/Electronic_Frontier_Foundation) (EFF) filed a [class action](http://en.wikipedia.org/wiki/Class_action) lawsuit against the NSA and several high-ranking officials of the [Bush administration](http://en.wikipedia.org/wiki/Presidency_of_George_W._Bush), charging an "illegal and unconstitutional program of dragnet communications surveillance," based on documentation provided by former [AT&T](http://en.wikipedia.org/wiki/AT%26T) technician [Mark Klein](http://en.wikipedia.org/wiki/Mark_Klein).

### AT&T Internet monitoring

Further information: [Hepting v. AT&T](http://en.wikipedia.org/wiki/Hepting_v._AT%26T), [Jewel v. NSA](http://en.wikipedia.org/wiki/Jewel_v._NSA), [Mark Klein](http://en.wikipedia.org/wiki/Mark_Klein), [NSA warrantless surveillance controversy](http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy)

In May 2006, [Mark Klein](http://en.wikipedia.org/wiki/Mark_Klein), a former [AT&T](http://en.wikipedia.org/wiki/AT%26T_Inc.) employee, alleged that his company had cooperated with NSA in installing [Narus](http://en.wikipedia.org/wiki/Narus_%28company%29) hardware to replace the FBI [Carnivore](http://en.wikipedia.org/wiki/Carnivore_%28software%29) program, to monitor network communications including traffic between American citizens.

### Domestic surveillance under Barack Obama

In 2009 the NSA intercepted the communications of American citizens, including a Congressman, although the [Justice Department](http://en.wikipedia.org/wiki/United_States_Department_of_Justice) believed that the interception was unintentional. The Justice Department then took action to correct the issues and bring it into compliance with existing laws. United States Attorney General [Eric Holder](http://en.wikipedia.org/wiki/Eric_Holder) resumed the wiretapping according to his understanding of the [Foreign Intelligence Surveillance Act](http://en.wikipedia.org/wiki/Foreign_Intelligence_Surveillance_Act) amendment of 2008, without explaining what had occurred.

On April 25, 2013, the NSA obtained a court order requiring [Verizon](http://en.wikipedia.org/wiki/Verizon)'s Business Network Services to provide information on all calls in its system to the NSA "on an ongoing daily basis", as reported by [*The Guardian*](http://en.wikipedia.org/wiki/The_Guardian) on June 6, 2013. This information includes "the numbers of both parties on a call ... location data, call duration, unique identifiers, and the time and duration of all calls" but not "[t]he contents of the conversation itself".

## International activity

### Criticism

[Edward Snowden](http://en.wikipedia.org/wiki/Edward_Snowden) revealed in June 2013 that between 8 February and 8 March 2013 NSA collected about 124.8 billion telephone data items and 97.1 billion computer data items throughout the world, including in [Germany](http://en.wikipedia.org/wiki/Germany), [United Kingdom](http://en.wikipedia.org/wiki/United_Kingdom) and [France](http://en.wikipedia.org/wiki/France). NSA made 70.3 million recordings of [French](http://en.wikipedia.org/wiki/France) citizens' [telephone](http://en.wikipedia.org/wiki/Telephone) data from 10 December 2012 to 8 January 2013.

## Role in scientific research and development

NSA has been involved in debates about public policy, both indirectly as a behind-the-scenes adviser to other departments, and directly during and after [Vice Admiral Bobby Ray Inman](http://en.wikipedia.org/wiki/Bobby_Ray_Inman)'s directorship. NSA was a major player in the debates of the 1990s regarding the [export of cryptography in the United States](http://en.wikipedia.org/wiki/Export_of_cryptography_in_the_United_States). Restrictions on export were reduced but not eliminated in 1996.

Its secure government communications work has involved the NSA in numerous technology areas, including the design of specialized communications [hardware](http://en.wikipedia.org/wiki/Computer_hardware) and software, production of dedicated [semiconductors](http://en.wikipedia.org/wiki/Semiconductor) (at the [Ft. Meade](http://en.wikipedia.org/wiki/Fort_Meade%2C_Maryland) chip fabrication plant), and advanced [cryptography](http://en.wikipedia.org/wiki/Cryptography) research. For 50 years, NSA designed and built most of its computer equipment in-house, but from the 1990s until about 2003 (when the U.S. Congress curtailed the practice), the agency contracted with the private sector in the fields of research and equipment.

### Data Encryption Standard

Main article: [Data Encryption Standard](http://en.wikipedia.org/wiki/Data_Encryption_Standard)





[FROSTBURG](http://en.wikipedia.org/wiki/FROSTBURG) was the NSA's first [supercomputer](http://en.wikipedia.org/wiki/Supercomputer), used from 1991–97.

NSA was embroiled in some minor controversy concerning its involvement in the creation of the Data Encryption Standard (DES), a standard and public [block cipher](http://en.wikipedia.org/wiki/Block_cipher) [algorithm](http://en.wikipedia.org/wiki/Algorithm) used by the [U.S. government](http://en.wikipedia.org/wiki/U.S._government) and banking community. During the development of DES by [IBM](http://en.wikipedia.org/wiki/IBM) in the 1970s, NSA recommended changes to some details of the design. There was suspicion that these changes had weakened the algorithm sufficiently to enable the agency to eavesdrop if required, including speculation that a critical component—the so-called [S-boxes](http://en.wikipedia.org/wiki/S-box)—had been altered to insert a "[backdoor](http://en.wikipedia.org/wiki/Backdoor_%28computing%29)" and that the reduction in key length might have made it feasible for NSA to discover DES keys using massive computing power. It has since been observed that the S-boxes in DES are particularly resilient against [differential cryptanalysis](http://en.wikipedia.org/wiki/Differential_cryptanalysis), a technique which was not publicly discovered until the late 1980s, but which was known to the IBM DES team. The [United States Senate Select Committee on Intelligence](http://en.wikipedia.org/wiki/United_States_Senate_Select_Committee_on_Intelligence) reviewed NSA's involvement, and concluded that while the agency had provided some assistance, it had not tampered with the design. In late 2009 NSA declassified information stating that "NSA worked closely with IBM to strengthen the algorithm against all except brute force attacks and to strengthen substitution tables, called S-boxes. Conversely, NSA tried to convince IBM to reduce the length of the key from 64 to 48 bits. Ultimately they compromised on a 56-bit key."

### Clipper chip

Main article: [Clipper chip](http://en.wikipedia.org/wiki/Clipper_chip)

Because of concerns that widespread use of strong cryptography would hamper government use of [wiretaps](http://en.wikipedia.org/wiki/Telephone_tapping), NSA proposed the concept of [key escrow](http://en.wikipedia.org/wiki/Key_escrow) in 1993 and introduced the Clipper chip that would offer stronger protection than DES but would allow access to encrypted data by authorized law enforcement officials. The proposal was strongly opposed and key escrow requirements ultimately went nowhere. However, NSA's [Fortezza](http://en.wikipedia.org/wiki/Fortezza) hardware-based encryption cards, created for the Clipper project, are still used within government, and NSA ultimately declassified and published the design of the [Skipjack cipher](http://en.wikipedia.org/wiki/Skipjack_%28cipher%29) used on the cards.

### Advanced Encryption Standard

Main article: [Advanced Encryption Standard](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

The involvement of NSA in the selection of a successor to DES, the Advanced Encryption Standard (AES), was limited to hardware performance testing (see [AES competition](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard_process)). NSA has subsequently certified AES for protection of classified information (for at most two levels, e.g. SECRET information in an unclassified environment) when used in NSA-approved systems.

### SHA

The widely used [SHA-1](http://en.wikipedia.org/wiki/SHA-1) and [SHA-2](http://en.wikipedia.org/wiki/SHA-2) hash functions were designed by NSA. SHA-1 is a slight modification of the weaker [SHA-0](http://en.wikipedia.org/wiki/SHA-0) algorithm, also designed by NSA in 1993. This small modification was suggested by NSA two years later, with no justification other than the fact that it provides additional security. An attack for SHA-0 that does not apply to the revised algorithm was indeed found between 1998 and 2005 by academic cryptographers. Because of weaknesses and key length restrictions in SHA-1, NIST deprecates its use for [digital signatures](http://en.wikipedia.org/wiki/Digital_signature), and approves only the newer SHA-2 algorithms for such applications from 2013 on.

A new hash standard, [SHA-3](http://en.wikipedia.org/wiki/SHA-3), has recently been selected through the [competition](http://en.wikipedia.org/wiki/NIST_hash_function_competition) concluded October 2, 2012 with the selection of [Keccak](http://en.wikipedia.org/wiki/SHA-3) as the algorithm. The process to select SHA-3 was similar to the one held in choosing the AES, but some doubts have been cast over it, since fundamental modifications have been made to Keccac in order to turn it into a standard. These changes potentially undermine the cryptanalisis performed during the competition and reduce the security levels of the algorithm.

### Dual\_EC\_DRBG random number generator

Main article: [Dual\_EC\_DRBG](http://en.wikipedia.org/wiki/Dual_EC_DRBG)

NSA promoted the inclusion of a random number generator called [Dual\_EC\_DRBG](http://en.wikipedia.org/wiki/Dual_EC_DRBG) in the U.S. [National Institute of Standards and Technology](http://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology)'s 2007 guidelines. This led to speculation of a [backdoor](http://en.wikipedia.org/wiki/Backdoor_%28computing%29) which would allow NSA access to data encrypted by systems using that pseudo random number generator.

This is now deemed to be plausible based on the fact that knowing future values of the internal state is possible if the relation between two internal elliptic curve points are known. Both NIST and RSA are now officially recommending against the use of this PRNG.

### Perfect Citizen

Main article: [Perfect Citizen](http://en.wikipedia.org/wiki/Perfect_Citizen)

Perfect Citizen is a program to perform vulnerability assessment by the NSA on U.S. critical infrastructure. It was originally reported to be a program to develop a system of sensors to detect cyber attacks on critical infrastructure computer networks in both the private and public sector through a network monitoring system named Einstein. It is funded by the [Comprehensive National Cybersecurity Initiative](http://en.wikipedia.org/wiki/Comprehensive_National_Cybersecurity_Initiative) and thus far Raytheon has received a contract for up to $100 million for the initial stage.

### Academic research

NSA has invested many millions of dollars in academic research under grant code prefix *MDA904*, resulting in over 3,000 papers (as of 2007-10-11). NSA/CSS has, at times, attempted to restrict the publication of academic research into cryptography; for example, the [Khufu and Khafre](http://en.wikipedia.org/wiki/Khufu_and_Khafre) block ciphers were voluntarily withheld in response to an NSA request to do so. In response to a [FOIA](http://en.wikipedia.org/wiki/Freedom_of_information_in_the_United_States) lawsuit, in 2013 the NSA released the 643-page research paper titled, "Untangling the Web: A Guide to Internet Research, " written and compiled by NSA employees to assist other NSA workers in searching for information of interest to the agency on the public Internet.

### Patents

NSA has the ability to file for a patent from the [U.S. Patent and Trademark Office](http://en.wikipedia.org/wiki/U.S._Patent_and_Trademark_Office) under [gag order](http://en.wikipedia.org/wiki/Gag_order). Unlike normal patents, these are not revealed to the public and do not expire. However, if the Patent Office receives an application for an identical patent from a third party, they will reveal NSA's patent and officially grant it to NSA for the full term on that date.

One of NSA's published patents describes a method of [geographically locating](http://en.wikipedia.org/wiki/Geolocation) an individual computer site in an Internet-like network, based on the [latency](http://en.wikipedia.org/wiki/Lag) of multiple network connections. Although no public patent exists, NSA is reported to have used a similar locating technology called trilateralization that allows real-time tracking of an individual’s location, including altitude from ground level, using data obtained from cellphone towers.





*Behind the Green Door* secure communications center with [SIPRNET](http://en.wikipedia.org/wiki/SIPRNET), GWAN, [NSANET](http://en.wikipedia.org/wiki/NSANET), and [JWICS](http://en.wikipedia.org/wiki/JWICS) access

## NSANet

NSANet is the official National Security Agency intranet. It is a classified internal network, and [TS](http://en.wikipedia.org/wiki/Top_secret)/[SCI](http://en.wikipedia.org/wiki/Sensitive_Compartmented_Information). In 2004 it was reported to have used over twenty [commercial off-the-shelf](http://en.wikipedia.org/wiki/Commercial_off-the-shelf) operating systems. Some universities that do highly sensitive research are allowed to connect to it. In 1998 it, along with [NIPRNET](http://en.wikipedia.org/wiki/NIPRNET) and [SIPRNET](http://en.wikipedia.org/wiki/SIPRNET), had "significant problems with poor search capabilities, unorganized data and old information".

## National Computer Security Center

The DoD Computer Security Center was founded in 1981 and renamed the National Computer Security Center (NCSC) in 1985. NCSC was responsible for computer security throughout the federal government. NCSC was part of NSA, and during the late 1980s and the 1990s, NSA and NCSC published [Trusted Computer System Evaluation Criteria](http://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria) in a six-foot high [Rainbow Series](http://en.wikipedia.org/wiki/Rainbow_Series) of books that detailed trusted computing and network platform specifications. The Rainbow books were replaced by the [Common Criteria](http://en.wikipedia.org/wiki/Common_Criteria), however, in the early 2000s.

On July 18, 2013, Greenwald alleged that Snowden held the blueprints of the National Computer Security Center, thereby sparking fresh controversy.

## NSA encryption systems

Main article: [NSA encryption systems](http://en.wikipedia.org/wiki/NSA_encryption_systems)

The NSA is responsible for the encryption-related components in these legacy systems:

* [FNBDT](http://en.wikipedia.org/wiki/FNBDT) Future Narrow Band Digital Terminal
* [KL-7](http://en.wikipedia.org/wiki/KL-7) ADONIS off-line rotor encryption machine (post-WWII – 1980s)
* [KW-26](http://en.wikipedia.org/wiki/KW-26) ROMULUS electronic in-line teletypewriter encryptor (1960s–1980s)
* [KW-37](http://en.wikipedia.org/wiki/KW-37) JASON fleet broadcast encryptor (1960s–1990s)





[STU-III](http://en.wikipedia.org/wiki/STU-III) secure telephones on display at the [National Cryptologic Museum](http://en.wikipedia.org/wiki/National_Cryptologic_Museum)

* [KY-57](http://en.wikipedia.org/wiki/KY-57) VINSON tactical radio voice encryptor
* [KG-84](http://en.wikipedia.org/wiki/KG-84) Dedicated Data Encryption/Decryption
* [STU-III](http://en.wikipedia.org/wiki/STU-III) secure telephone unit, phased out by the [STE](http://en.wikipedia.org/wiki/Secure_Terminal_Equipment)

The NSA oversees encyption in following systems which are in use today:

* [EKMS](http://en.wikipedia.org/wiki/EKMS) Electronic Key Management System
* [Fortezza](http://en.wikipedia.org/wiki/Fortezza) encryption based on portable crypto token in [PC Card](http://en.wikipedia.org/wiki/PC_Card) format
* [SINCGARS](http://en.wikipedia.org/wiki/SINCGARS) tactical radio with cryptographically controlled frequency hopping
* [STE](http://en.wikipedia.org/wiki/Secure_Terminal_Equipment) secure terminal equipment
* [TACLANE](http://en.wikipedia.org/wiki/TACLANE) product line by [General Dynamics C4 Systems](http://en.wikipedia.org/wiki/General_Dynamics_C4_Systems)

The NSA has specified [Suite A](http://en.wikipedia.org/wiki/NSA_Suite_A_Cryptography) and [Suite B](http://en.wikipedia.org/wiki/NSA_Suite_B_Cryptography) cryptographic algorithm suites to be used in U.S. government systems; the Suite B algorithms are a subset of those previously specified by [NIST](http://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) and are expected to serve for most information protection purposes, while the Suite A algorithms are secret and are intended for especially high levels of protection.

## See also

* [Government Communications Security Bureau](http://en.wikipedia.org/wiki/Government_Communications_Security_Bureau) GCSB - New Zealand
* [Gulf of Tonkin incident](http://en.wikipedia.org/wiki/Gulf_of_Tonkin_incident)
* [Korean Air Lines Flight 007](http://en.wikipedia.org/wiki/Korean_Air_Lines_Flight_007)
* [NSA in popular culture](http://en.wikipedia.org/wiki/NSA_in_popular_culture)
* [Operation Ivy Bells](http://en.wikipedia.org/wiki/Operation_Ivy_Bells)
* [Special Communications Service of Russia](http://en.wikipedia.org/wiki/Special_Communications_Service_of_Russia) - Spetssvyaz
* [National Intelligence Priorities Framework](http://en.wikipedia.org/wiki/National_Intelligence_Priorities_Framework)

This page was last modified on 7 November 2013 at 10:18.