



10 Sep 2010

## CLOSE ACCESS SIGADS

## Close Access SIGADs

-----

All Close Access domestic collection uses the US-3136 SIGAD with a unique two-letter suffix for each target location and mission. Close Access overseas GENIE collection has been assigned the US-3137 SIGAD with a two-letter suffix.

(Note: Targets marked with an \* have either been dropped or are slated to be dropped in the near future. Please check with TAO/RTD/ROS [REDACTED] regarding authorities status.)

SIGAD Suffix	US-3136 Target/Country	Location	Covert term	Mission
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
OF	France/UN	New York	BLACKFOOT	HIGHLANDS
VC	France/UN	New York	BLACKFOOT	VAGRANT
UC	France/Emb	Wash, DC	WABASH	HIGHLANDS
LO	France/Emb	Wash, DC	WABASH	PBX

## General Term Descriptions

-----

HIGHLANDS: Collection from Implants  
 VAGRANT: Collection of Computer Screens  
 MAGNETIC: Sensor Collection of Magnetic Emanations  
 MINERALIZE: Collection from LAN Implant  
 OCEAN: Optical Collection System for Raster-Based Computer Screens  
 LIFESAVER : Imaging of the Hard Drive  
 GENIE: Multi-stage operation; jumping the airgap etc.  
 BLACKHEART Collection from an FBI Implant  
 PBX Public Branch Exchange Switch

Derived From: NSA/CSSM 1-52

Dated: 20041123

Declassify On: 20291123

CRYPTO ENABLED Collection derived from AO's efforts to enable crypto  
DROPMIRE: passive collection of emanations using an antenna  
CUSTOMS Customs opportunities (not LIFESAVER)  
DROPMIRE Laser printer collection, purely proximal access (\*\*NOT\*\*  
implanted)  
DEWSWEEPER USB (Universal Serial Bus) hardware host tap that provides  
COVERT link over USB link into a target network.  
Operates w/RF relay subsystem to provide wireless  
Bridge into target network.  
RADON Bi-directional host tap that can inject Ethernet packets onto the  
same target. Allows bi-directional exploitation of  
Denied networks using standard on-net tools.

## Document interne de la NSA sur l'espionnage visant la France

2 pages - Contributed by Martin Untersinger , Le Monde - Oct 18, 2013

Ce terme désigne la classification utilisée par la NSA pour répertorier ses dispositifs d'interception et de surveillance. (p. 1)

IGADs

Les programmes visant la France sont décrits un peu plus bas sur la page. (p. 1)

HIGHLANDS  
VAGRANT  
HIGHLANDS  
PBX

Descriptions des techniques d'interception (p. 1)

General Term Descriptions

Il s'agit de la liste des techniques utilisées de manière générale par la NSA pour son espionnage, et non de celles visant spécifiquement la France. Les techniques utilisées contre la France portent le nom de Highland, Vagrant et PBX.

## [International](#) » [World](#)

### NSA planted bugs at Indian missions in D.C., U.N.

Shobhan Saxena



The NSA selected India's U.N. office and the embassy as "location target" for infiltrating with hi-tech bugs, which might have given them access to vast quantities of Internet traffic. File photo. AP

***They were penetrated by NSA bugs that can copy entire hard disks***

Two of the most important nerve-centres of Indian diplomacy outside the country — the Permanent Mission of India at the United Nations and the embassy in Washington, DC — were targets of such sophisticated bugs implanted by the U.S. National Security Agency (NSA) that entire computer hard disks might have been copied by the American agency. The U.N. Mission building in New York and the embassy premises, including its annex, in Washington were on a top-secret list of countries and missions — many of them European allies of the U.S. — chosen for intensive spying.

According to a top-secret NSA document obtained by *The Hindu*, the NSA selected India's U.N. office and the embassy as "location target" for infiltrating their computers and telephones with hi-tech bugs, which might have given them access to vast quantities of Internet traffic, e-mails, telephone and office conversations and even official documents stored digitally.

Since the NSA revelations began in June, U.S. President Barack Obama and other top American officials have all claimed that the surveillance activities were aimed exclusively at preventing terrorist attacks. But the targeted spying of Indian diplomatic buildings could have been done for political and commercial reasons — not the core responsibility of the NSA.

According to the 2010 COMINT (communication intelligence) document about "Close Access SIGADs", the offices of Indian diplomats and high-ranking military officials stationed at these important posts were targets of four different kinds of electronic snooping devices:

Lifesaver, which facilitates imaging of the hard drive of computers

Highlands, which makes digital collection from implants

Vagrant, which collects data of open computer screens, and

Magnetic, which is a collection of digital signals

All the Indian "targets" in the list are marked with an asterisk, which, according to the document, means that they "have either been dropped or are slated to be dropped in the near future." The NSA document doesn't say when and how the bugs were implanted or how much of data was lifted from Indian offices, but all of them were on the "target" list for more than one type of data collection bugs.

Asked by *The Hindu*, why India's U.N. mission and embassy, which clearly pose no terrorism threat to the U.S., were targeted by the NSA, a spokesman for the Office of the Director of National Intelligence said: "The U.S. government will respond through diplomatic channels to our partners and allies. While we are not going to comment publicly on every specific alleged intelligence activity, as a matter of policy we have made clear that the United States gathers foreign intelligence of the type gathered by all nations. We value our cooperation with all countries on issues of mutual concern."

But the spokesman didn't answer *The Hindu's* specific questions about why the top-secret document about spying on Indian missions shouldn't be revealed or "reproduced by this newspaper in full or part".

The document obtained by *The Hindu* reveals a scary scenario of breach of official secrecy of Indian missions and violation of privacy of Indian diplomats and other staff working in the three premises that were targeted.

Located between 2nd and 3rd Avenue on 43rd Street in the eastern part of Manhattan, the office of India's permanent representative to the UN was on top of the list of Indian targets. Designed by the legendary Indian architect, Charles Correa, the building with a red granite base and a double-height penthouse porch at the top has the offices of India's permanent representative, deputy permanent representative, a minister and political coordinator, six counsellors, a Colonel-rank military advisor and several other secretaries who look after different areas of India's engagement with the world.

It was this building that was the main target of all four NSA bugs: from Lifesaver, which can send to the NSA copies of everything saved on the hard drives of office computers, to Vagrant, which can pick data straight from computer screens.

Though emails sent to India's New York mission have remained unanswered so far, an Indian diplomat told *The Hindu* that the NSA eavesdropping might have done "extensive damage" to India's stand on many international issues ranging from UN Security Council reforms to peacekeeping operations. "If they could implant bugs inside communications equipment of European Union office here and tap into their communications cables as well, there is no reason to believe that they didn't snoop on us," said the diplomat, speaking strictly on condition of anonymity. "We are still assessing the damage. If they managed to copy our hard drives, nothing is left to imagination."

Second to the UN mission on the "target" list was the chancery building of the Indian Embassy located at 2107, Massachusetts Avenue in Washington, DC. Consisting of two adjacent buildings, one constructed in 1885 and the other in 1901, the chancery has offices of the Indian ambassador, the deputy chief of mission, several ministers and counsellors who head political, economic, defence and industry sections and three Defence Attachés representing the Indian Army, Air Force and Navy. This building, from where India maintains its diplomatic, trade and strategic ties with the U.S., was on the "target" list for three bugs that can make images of hard drives, pick digital signals and copy data of computer screens.

The third Indian building targeted by the NSA is the embassy annex located on 2536, Massachusetts Avenue in Washington, DC. The annex has three very important departments: the consular section, headed by a minister, looks after visa services; the commerce department, also headed by a minister, is involved in a broad range of trade issues and negotiations besides assisting the Indian businesses; and an office of the Indian Space Research Organization (ISRO), represented by a counsellor, takes care of cooperation between two countries in the field of space. This building was on the NSA "target" list for Highlands and Vagrant, which collect data from implants and computer screens respectively. It's important to recall here that India's space programme was targeted by another NSA tool PRISM, which intercepts and collects actual content on internet and telephone networks (as reported by *The Hindu* on Tuesday).

But officials at the Indian embassy claim that the premises are safe. "Adequate measures are in place in this regard and all steps taken to safeguard the national interest," wrote an official in an email response to queries by *The Hindu*. Though no Indian official was willing to talk on record specifically about the NSA bugs mentioned in the top secret document, in private they admitted that it's a violation of all norms and security. "If these bugs were implanted physically on our machinery, telephones and computers, it means a serious breach in security. Who did that job for them? It's very alarming situation. Even if they accessed our data remotely, it is quite a serious matter because we try to de-bug our systems constantly," said an Indian diplomat, speaking on condition of anonymity.

The document obtained by *The Hindu* doesn't say if the bugs were placed physically or if the machines at the Indian Mission and embassy were targeted through the internet network, bugs similar to those aimed at Indian offices were actually "implanted" in a commercially available encrypted fax machine used at missions such as that of the European Union. In a recent expose, *The Guardian* had revealed that the NSA infiltrated the internal computer network of several European embassies and the EU to intercept their communications. That had led to a roar of protests from European capitals.

Alarm bells have been ringing in New Delhi too since July when it was first reported that 38 embassies and diplomatic missions, including the Indian embassy in Washington, were targeted by the NSA. Reacting to the reports, the Ministry of External Affairs spokesperson Syed Akbaruddin had expressed concern at the “disconcerting” reports and said that the government would take up the concern with the Americans. But at that time, the Indian government was neither aware of the fact that the UN mission in New York too was a “target” of NSA bugging nor did the officials know a thing about the nature and capabilities of the bugs used for snooping on their offices.

The Indian mission to the UN has so far not reacted to either the reports of snooping on foreign missions nor to The Hindu’s queries sent to its office in New York, but the embassy officials have discussed the issue with their American counterparts. “Our government has expressed concerns over the reports of monitoring of the Indian Embassy in Washington, D.C. by U.S. agencies, and the Embassy in Washington D.C. has raised these concerns with the U.S. government,” said an embassy official in an email repose to The Hindu’s queries, without elaborating at what level and in which meeting the issue was raised or what was the response of American officials.

But the U.S. officials have already made it clear that they would not “apologise” to anyone for the bugging of foreign mission, including the Indian embassy and New York office, as shown in NSA documents. “While we’re not going to comment publicly on the specifics of alleged intelligence activities, as a matter of policy we’ve made clear that the U.S. gathers foreign intelligence of the type gathered by all nations,” U.S. State Department spokesman Patrick Ventrell had told reporters at his daily news conference on July 2, a day after the spying on European embassies was revealed for the first time in reports where India was just mentioned in a passing reference.

Keywords: [DIA](#), [NSA snooping](#), [US surveillance programme](#), [National Security Agency](#), [Prism](#), [Freedom of Information Act](#)