PRIVACY INTERNATIONAL

Tipping the scales: Security & surveillance in Pakistan

Special Report

Tipping the scales: Security & surveillance in Pakistan

July 2015

PRIVACY INTERNATIONAL

www.privacyinternational.org

Executive Summary

The Pakistani government is engaged in a protracted conflict against armed militant groups within its borders and outside its borders, it is a key player in the global 'war on terror'. Communications surveillance - of phone and internet protocol (IP) traffic, domestically and internationally - and other forms such as biometric or device registration, is justified by the government as necessary to counter these internal and external threats, even as it becomes less and less targeted and more widespread against ordinary civilians. The military's defence budget has ballooned in recent years as result of significant levels of international assistance, with the military's access to sophisticated technologies having increased in turn. Attacks against civilian targets in Pakistan's cities have also fed popular support for communications surveillance and other efforts to register and monitor the civilian population, including national databases and mandatory SIM card registration.

Pakistan's intelligence agencies have abused their communications surveillance powers, including by spying on opposition politicians and Supreme Court judges. Widespread internet monitoring and censorship has also been used to target journalists, lawyers and activists.

This report outlines the state of communications surveillance in Pakistan. It compares the vague and imprecise laws that govern it against international human rights law standards. The report also gives an overview of the international intelligence operations that Pakistan has participated in and been subject to, including programmes operated by the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ).

This report reveals, through confidential previously never before released documents, that in 2013 the Inter-Services Intelligence, Pakistan's best known intelligence agency, sought to commission a mass surveillance system to tap international undersea cables at three cable landing sites in southern Pakistan. The "Targeted IP Monitoring System and COE [Common Operations Environments]" would allow Pakistan to collect and analyse a significant portion of communications travelling within and through the country at a centralized command centre. With a projected intake of an estimated 660 gigabytes per second, the system would amount to a significant expansion of Pakistan's communications intelligence gathering capacities.

Through investigation and analysis of the private surveillance industry's role in Pakistan by Privacy International, the report shows that mass network surveillance has been in place in Pakistan since at least 2005. The Pakistani government obtained this technology from both domestic and foreign surveillance companies including Alcatel, Ericsson, Huawei, SS8 and Utimaco.

This report reveals for the first time some of the previously unknown surveillance capacities of the Pakistani government. It also finds that the practical capacity of the Pakistani government, particularly the Inter-Services Intelligence Agency, now outstrips the capacity of domestic and international law for effective regulation of that surveillance. This report contains recommendations for how Pakistan might move away from its current surveillance model to one that complies with applicable human rights law standards, and, as such, no longer represents a threat to Pakistani democracy.

Recommendations

To the Pakistan Senate Defence Committee:

- Convene an inquiry into the 2013 ISI call for proposals entitled "GSR for Targeted IP Monitoring System and COE". This inquiry should request information on any discussion prior to the proposal in 2013 of the adequacy, legality, necessity and proportionality of the proposed project.
- Conduct an investigation into the NSA's surveillance of Pakistan communication networks, including the legality of these actions and the extent and nature of data-sharing arrangements between the NSA and Pakistani intelligence agencies.
- Conduct an investigation into GCHQ's alleged access to the Pakistan Internet Exchange.

To the Review Committee established under Section 27, Investigation for Fair Trial Act, 2013:

- Release consolidated data regarding number of applications for warrants for communications surveillance under the Investigation for Fair Trial Act.
- Declassify and release any "orders or instructions" given by the Review Committee to the intelligence agencies under Section 27 (2) of Investigation for Fair Trial Act, 2013.

To foreign governments and export control authorities:

- Commit to and implement agreements on export control measures related to electronic surveillance technologies.
- Ensure strong human rights criteria are included in export control provisions that are specific to surveillance technologies; these should take into account national legal frameworks, oversight mechanisms, and the end-user's record of using electronic surveillance.
- Identify products that can be subject to export licensing without harming security research or otherwise negatively impacting the development of the information and communications technology sector. Measures could include the addition of a product to a national or multilateral export control regime control list and end-use and end-user stipulations.
- Work within export control regimes, and with multilateral institutions, and other states to identify and mitigate challenges to applying and enforcing export control regulations on surveillance technologies, particularly regarding brokering, re-export, incorporation, and diversion challenges.
- Adopt legislation conditioning financial or technical assistance, transfer of equipment, or sharing of intelligence to/with law enforcement, military, or intelligence agencies in foreign countries on strong human rights provisions. Such provisions must explicitly prohibit any support for individuals or agencies proven or strongly suspected to be involved in human rights violations.
- Carry out an extensive audit of security assistance that has been provided to Pakistani law enforcement, military, or intelligence agencies since 2000 to ascertain if any such assistance has led to human rights violations.
- Publicly disclose all form of security assistance to Pakistan, including details regarding financial or technical assistance, transfer of equipment, or sharing of intelligence with law enforcement, military or intelligence agencies.
- Adopt strong end-use monitoring mechanisms regarding security assistance provided to foreign countries via, but not limited to, diplomatic channels and engagement with civil society and multilateral institutions.
- Publicly disclose any such end-use monitoring mechanisms and publish, on an annual basis, the results of any such monitoring of security assistance.

To foreign companies selling communications surveillance equipment:

- Carry out due diligence and 'Know Your Customer' research on any potential beneficial end-users prior to agreeing to a potential transaction.
- Do not export a product if the beneficial end-user of the product cannot be clearly identified or where there is a documented record of human rights abuse in the country to which you are considering selling your product.
- Stipulate clear end-use assurances in contractual agreements with customers encompassing strong human rights safeguards and protecting against their arbitrary or unlawful use.
- Carry out a periodic review of states' use of the technology you have sold them, and refuse to carry out maintenance, training, or updates if the end-use does not conform to these contractual obligations.
- Original Equipment Manufacturers (OEM) should ensure that the company incorporating their equipment adheres to export control regulations and to the OEM's own human rights provisions.

Politics and surveillance in Pakistan

Pakistan's sizeable population generates huge amounts of communications traffic. Over 70 per cent of its population of 180 million have mobile phone subscriptions, and an estimated 11% of the population uses the internet[1]. Fifty operational internet providers[2] and five mobile operators[3] serve this demand.

Surveillance of communications across these networks is technologically advanced and comprehensive. Pakistan's important geopolitical role countering insurgent and Islamist groups has resulted in the Pakistani military and intelligence establishment receiving high levels of funding from overseas governments to develop advanced communications surveillance infrastructure. Relevant agencies within the Pakistani government have moved toward the mass capture and storage of communications of ordinary citizens, whereas previously they had mainly used tactical military surveillance tools, which are far more targeted.

Popular support for surveillance of communications is high in Pakistan. Intermittent devastating attacks within Pakistan's major cities by insurgent groups, such as the 2014 Peshawar school attack by a Taliban-affiliated group, have been cited as a reason to expand surveillance in Pakistan[4].

Intelligence functions are dispersed across a number of government agencies that collect and/or use intercepted communications. Each branch of the Pakistani armed forces has its own intelligence service conducting signals intelligence. Other agencies include the Inter-Services Intelligence (ISI) and Joint Signal Intelligence Bureau. The Ministry of Justice is responsible for the Federal Investigation Agency and others that use intercepted communications data for criminal investigation and prosecution. Under the Ministry of Science and Technology, the Joint Intelligence Technical and Joint Intelligence X units carry out a number of surveillance research and development functions. The Intelligence Bureau, under the Prime Minister, has also used intercepted communications data.

The capacity for mass automated interception of ordinary citizens' communications has been expanded and framed as an essential condition for ensuring citizens' security[5]. Registration of personal data is widespread and enjoys a high level of popular support. SIM cards must be registered to their user[6]. Unlike in most countries with mandatory registration, SIM cards are also biometrically verified against the National Database and Registration Authority's (NADRA)[7] national database[8], often by fingerprint[9].

1 According to the World Bank (2013 data). "Pakistan: Internet users (per 100 people)", The World Bank, 2013 http://databank.worldbank.org/data//reports.aspx?source=2&country=PAK&series=&period=

2 "Pakistan's Internet Landscape", Bytes for All Pakistan, November 2013, http://content.bytesforall.pk/sites/default/files/MappingReportFinal%20-%20Published.pdf

3 "Cellular Mobile", Pakistan Telecommunications Authority (PTA), 28 March 2014, http://www.pta.gov.pk/index.php?Itemid=135

4 See, for example, "After Peshawar: Reassessing the terror threat", DAWN, 18 December 2014, http://www.dawn.com/news/1151616

5 "'Fair trial bill' passed in big compromise", DAWN, 20 December 2012, http://www.dawn.com/news/772798/fair-trial-bill-passed-in-big-compromise

6 "Pakistani SIM users given until 17 May to register", Telegeography, 27 April 2011, https://www.telegeography.com/products/commsupdate/articles/2011/04/27/pakistani-sim-users-given-until-17-may-to-register/

7 "Pakistani SIM users given until 17 May to register", Telegeography, 27 April 2011, https://www.telegeography.com/products/commsupdate/articles/2011/04/27/pakistani-sim-users-given-until-17-may-to-register/

8 "National Action Plan: 53 million SIMs verified via biometric system", Pakistan Today, 22 February 2015, http://www.pakistantoday.com.pk/2015/02/22/national/national-action-plan-53-million-sims-verified-via-biometric-system/

9 "Pakistan's mobile phone owners told: be fingerprinted or lose your sim card", The Guardian, 3 March 2015, http://www.theguardian.com/world/2015/mar/03/pakistan-fingerprint-mobile-phone-users?

Pakistan has one of the world's most extensive citizen registration regimes – over 96 % of citizens reportedly have biometric ID cards[10], including the Smart National Identity Card (SNIC)[11], which contains its owner's biometric photo, a computer chip, address and parental information. ID cards are commonly required to access services ranging from opening a bank account to getting a passport. Nevertheless, serious misidentification errors can occur[12] and forgery is rife[13].

Interception across Pakistani networks is pervasive; some of it is also unlawful. A Supreme Court hearing about a case concerning phone tapping revealed that the ISI tapped 6,523 phones in February, 6,819 in March and 6,742 in April 2015[14]. The case, dating from 1996, was brought following evidence that the then-Chief Justice's phone had been tapped. At time of publication, no details about the procedures and process for intercepting communications had yet been publicly released.

Since 2004 network providers have been required to comply with requests for interception and access to network data as a standard condition of the PTA's award of operating licenses to phone companies[15].

10 "Pakistan's experience with identity management", BBC News, 8 June 2012, http://www.bbc.co.uk/news/world-asia-18101385
11 "Solutions", National Database and Registration Authority (NADRA), 2015, https://www.nadra.gov.pk/index.php/solutions
12 "Pakistan's mobile phone owners told: be fingerprinted or lose your sim card", The Guardian, 3 March 2015, http://www.theguardian.com/world/2015/mar/03/pakistan-fingerprint-mobile-phone-users
13 "Identity theft persists in Pakistan's biometric era", Nighat Dad, Privacy International, 22 July 2014, https://www.privacyinternational.org/?q=node/334
14 "Phone-tapping: SC to take up ISI's plea for in-camera hearing on Wednesday", The Express Tribune, 16 June 2015, http://tribune.com.pk/story/904267/phone-tapping-sc-to-take-up-isis-plea-for-in-camera-hearing-on-wednesday/
15 "Mobile Cellular Policy " Pakistan Ministry of Information Technology , 28 January 2004, http://www.pakistan-law.com/mobilepolicy28012004.pdf

International surveillance cooperation

Pakistan cooperates heavily with international surveillance initiatives against its own citizens, particularly those led by the US National Security Agency (NSA). The Pakistani government is by far the largest known recipient of NSA funds.[16]

Pakistan is also one of the NSA's approved third party SIGINT partners. Being a third party partner means that the NSA considers the relationship a long-term one involving "higher degrees of trust" and "greater levels of cooperation" such that the NSA would be "willing to share advanced techniques…in return for that partner's willingness to do something politically risky." A third party partner can expect to receive "technical solutions (e.g. hardware or software) and/or access to related technology.[17]"

The NSA especially values its relationship with Pakistan. The NSA maintains a 'special collection service' at its embassy and consulates in Pakistan[18]. In 2008, it maintained at least one server in Pakistan for its programme XKeyscore, which searches and analyzes intercepted data. Under the Boundless Informant program, the NSA collected over 97 billion pieces of intelligence globally over a 30-day period ending in March 2013. Within this, Pakistan had the highest number of intercepted DNR (dialed number recognition) and second highest number of intercepted DNI (dialed number identification)[19]. Pakistan also featured strongly in the NSA's Fairview program.

Fairview is a mass surveillance programme designed to collect phone, internet and e-mail data in bulk from the computers and mobile telephones of foreign countries' citizens. NSA slides published in Brazil's O Globo show that in one month in 2012, for instance, the NSA analyzed 11.7 billion records of DNI traffic. of DNI traffic into and out of Pakistan, as well as traffic to top Pakistani domain names[20].

A June 2012 NSA document recently published, shows that the NSA, through its SKYNET programme, harvests call data from Pakistani telecommunications providers (though does not specify how) and that 55 million phone records were fed into an NSA analysis system for an analysis exercise. Known ISI agents were tracked in this experiment as well as an Al Jazeera journalist being misidentified as being a member of Al Qaeda.

Pakistan networks have also been targeted by the NSA's British counterpart,the Government Communications Headquarters (GCHQ). In 2010,[21] a joint unit of NSA and GCHQ hacked the world's largest producer of SIM cards, Gemalto. The breach, detailed in a secret 2010 GCHQ document, gave the surveillance agencies the potential to secretly monitor a large portion of the world's cellular communications, including both voice and data.

16 "FAD FY 12 CCP Funding of Partners", National Security Agency slide reproduced in Glenn Greenwald, No Place to Hide, p. 124. http://glenngreenwald.net/pdf/NoPlaceToHide-Documents-Compressed.pdf

17 "What are We After with Our Third Party Relationships – And What Do They Want from Us, Generally Speaking?" National Security Agency slide, 15 September 2009, https://s3.amazonaws.com/s3.documentcloud.org/documents/1084762/third-party-relationships.pdf

18 "Driver 1: Worldwide SIGINT/Defense Cryptologic Platform", National Security Agency slide reproduced in Glenn Greenwald, No Place to Hide, p. 117 http://us.macmillan.com/static/holt/greenwald/NoPlaceToHide-Documents-Compressed.pdf

19 "Boundless Informant: the NSA's secret tool to track global surveillance data", The Guardian, 11 June 2013, http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

20 The image can be found here, http://leandroamaral.blogspot.co.uk/2013/07/mapa-mostra-volume-de-rastreamento-do.html

21 "Boundless Informant: the NSA's secret tool to track global surveillance data", The Guardian, 11 June 2013, http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

GCHQ successfully identified the identifying information of tens of thousands of SIM cards in a number of countries.[22] However, GCHQ's automated key harvesting system failed to produce results against Pakistani networks. This is despite there being "priority targets" for the UK in Pakistan, and despite the fact that GCHQ had a store of 'Kis' keys from two major Pakistani providers, Mobilink and Telenor.[23] GCHQ has also hacked into the Pakistan Internet Exchange - a common point of transfer for a significant portion of Pakistanis' communications - as part of its Computer Network Exploitation operations, giving the spy agency "access to almost any user of the internet" inside Pakistan.[24]

The Pakistani government's reaction to revelations that foreign governments have engaged in mass surveillance of communications has been mixed. In 2013, Pakistani Senators expressed concern after initial revelations about the scale of NSA surveillance in Pakistan,[25] and in 2014, the Pakistani Foreign Office officially protested against the NSA's surveillance of its left-leaning political party, the Pakistan People's Party (PPP).[26] The Pakistani government have made few statements about the NSA's activities in Pakistan. In contrast, civil society in and out of Pakistan reacted vehemently to the revelations.[27]

22 "IMSIs identified with KI data for Network Providers Jan10-Mar10 Trial", National Security Agency slide published by The Intercept, 19 February 2015, https://firstlook.org/theintercept/document/2015/02/19/imsis-identified-ki-data-network-providers-jan10-mar10-trial/

23 "The Great SIM Heist: How spies stole the keys to the encryption castle", The Intercept, 19 February 2015, https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

24 "UK online snooping against Pakistan 'alarming'", Dawn, 24 June 2015, https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

25 "Report of the Senate Committee on Defence and Defence Production", Senate of Pakistan, August-September 2013, http://www.senate.gov.pk/uploads/documents/1378101374_113.pdf

26 "Pakistan lodges formal protest with US against PPP surveillance", DAWN, 6 July 2014, http://www.dawn.com/news/1116802

27 See for example "Pakistan responds to the NSA Surveillance of PPP", Digital Rights Foundation, 8 July 2014, http://digitalrightsfoundation.pk/2014/07/pakistan-responds-to-the-nsa-surveillance-of-ppp/ and "Press Freedom Groups Denounce NSA Spying on AJ Bureau Chief", Inter Press Service, 12 May 2015, http://www.ipsnews.net/2015/05/press-freedom-groups-denounce-nsa-spying-on-aj-bureau-chief/

Legal context governing interception

Pakistan, like almost every other nation in the world, has ratified the International Convention on Civil and Political Rights (ICCPR),[28] the leading international human rights treaty. Article 17 of the ICCPR stipulates that '[n]o one shall be subject to arbitrary or unlawful interference with his privacy, family or correspondence.'[29] The ICCPR also commits Pakistan to ensure the protection of those other rights that rely on the protection of privacy such as freedom of expression[30] and freedom of association.[31] Further, the Cairo Declaration on Human Rights in Islam, to which Pakistan is also a signatory, affirms in Article 18 that '[e]veryone shall have the right to privacy in the conduct of his private affairs, in his home, among his family,' and specifically sets out that '[i]t is not permitted to spy on him, to place him under surveillance or to besmirch his good name. The State shall protect him from arbitrary interference'.[32]

With respect to surveillance, the UN Human Rights Committee, a body of independent experts charged with interpreting the ICCPR, has clarified that any interference with rights via surveillance must, in order to be lawful, be carried out pursuant to legislation that 'specif[ies] in detail the precise circumstances in which such interferences may be permitted'[33]. Any such authorized interference with rights must occur 'only by the authority designated under the law, and on a case-by-case basis'.[34] Further, the UN Special Rapporteur on Freedom of Expression has similarly stated that '[c] ommunications surveillance should be regarded as a highly intrusive act' and that '[l] egislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority'.[35]

These standards reinforce the general requirement of international human rights law that states may only limit rights in exceptional circumstances. Limitations to privacy rights in Pakistan and other countries that are signatories to the ICCPR can only occur where those limitations are set out in clear and predictable domestic law, are applied in service of a small range of predetermined, legitimate aims, and proportionate to the legitimate aim pursued.[36] Based on its international legal commitments, Pakistan is obliged to refrain from broad surveillance programmes and to set out clearly in its domestic law the conditions which, if exceptional cases arise, limited interferences with privacy through targeted surveillance may be allowed.

Privacy is also a fundamental premise of Pakistan's domestic law. Article 14(1) of the Constitution confirms that '[t]he dignity of man and, subject to law, the privacy of home, shall be inviolable.' As a fundamental constitutional right, the right to privacy is meant to take precedence over any other inconsistent provisions of domestic law: Article 8 of the Constitution provides that '[a]ny law, or any custom or usage having the force of law, in so far as it is inconsistent with the rights conferred [under the Constitution], shall, to the extent of such inconsistency, be void.'

28 UN General Assembly, International Covenant on Civil and Political Rights, opened for signature 16 December 1966, entered into force 23 March 1976, 999 UNTS 171 ('ICCPR').
29 ICCPR, Article 17(1)
30 ICCPR, Article 19.
31 ICCPR, Article 22.
32 Organization of the Islamic Conference, Cairo Declaration on Human Rights in Islam, 5 August 1990, Article 18(b).
33 UN Human Rights Committee, General Comment 16, UN Doc. HRI/GEN/1/Rev.9(Vol 1) ('General Comment 16'), [8].
34 General Comment 16, [8].
35 UN Special Rapporteur on Freedom of Expression, Report (17 April 2013), UN Doc. A/HRC/23/40, [81].
36 See the Human Rights Committee decision in Mukong v Cameroon, UN Doc. CCPR/C/51/D/458/1991 (1994), [9.7].

Yet Pakistan's Constitution also includes a wide-ranging exception to the primacy of fundamental rights: the provisions of Article 8 do not apply to any law relating to the 'proper discharge' of the duties of the Armed Forces or the police.[37] The breadth of this exception is troubling, especially given the central role that the Armed Forces in particular have historically played in Pakistan's domestic political landscape.

Key legislative provisions raise serious concerns as to the strength of these supposed protections. The Anti-Terrorism Act (1997), for instance, specifically authorizes a wide range of officers to enter and search premises without a warrant upon reasonable suspicion of containing written material, recordings, property, or other articles in connection with terrorism.[38] There is no requirement for a warrant so long as a relevant officer can satisfy themselves that there exists a link to terrorism. No opportunity exists for independent oversight – accordingly, there is minimal opportunity to discover or guard against abuse.[39]

State surveillance in Pakistan is currently governed by the framework set out in the innocuously-named Investigation for Fair Trials Act (2013).[40] This act allows for access to data, emails, telephone calls, and any form of computer or mobile phone-based communication, subject to judicial warrant. However, a warrant can be requested wherever an official has 'reasons to believe' that a citizen is, or is 'likely to be associated' with, or even 'in the process of beginning to plan' an offence under Pakistani law. The breadth of those qualifying criteria is remarkable, and renders the additional protection offered by the process of applying to a judge illusory.

The Prevention of Electronic Crimes Bill (PECB) (2015) also threatens to erode privacy rights in Pakistan further. Currently awaiting consideration by the National Assembly and Senate, the PECB establishes mechanisms by which State officers may order the retention or provision of communications data (including from operators of communications networks).[41] While the officer is required to notify a court of these orders, the court has no role in vetting or reviewing the grounds, or of considering the necessity or proportionality of any action taken. These powers apply to communications data rather than the content of communications. Yet significant concerns remain about the bill's implications for citizens' privacy. Communications data allow 'very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained,' relating to personal associations, patterns of behaviour, and the like, as the Court of Justice of the European Union recently noted.[42]

37 Constitution of the Islamic Republic of Pakistan, Article 8(3)(a). National Assembly of Pakistan, 1973, http://www.pakistani.org/pakistan/constitution/part2.ch1.html

38 Anti-Terrorism Act 1997, ss5 and 10. National Assembly of Pakistan, 1997, http://www.ppra.org.pk/doc/anti-t-act.pdf

39 The Anti-Terrorism Act finds precedent in the Security of Pakistan Act (1952), which provides for control orders and sweeping entry, search, and confiscation powers wherever a government official (rather than a court) considers citizens or associations to come within the vague definition of 'acting in any manner prejudicial to the defence or external affairs or security of Pakistan.' Security of Pakistan Act 1952, ss3 and 10. 5, May 1952, http://pakistancode.gov.pk/pdf-file-pdffiles/admin4d89bd23fd7d2201bf1e4fb0dc7a29d8.pdf-apaUY2Fqa-ap%2BYZw%3D%3D

40 Investigation for Fair Trials Act, National Assembly of Pakistan, 22 February 2013, http://www.na.gov.pk/uploads/documents/1361943916_947.pdf

41 Prevention of Electronic Crimes Bill 2015, Limited Circulation Draft, ss28 and 29. National Assembly Standing Committee, http://bolobhi.org/wp-content/uploads/2015/04/NA-Standing-Committee-Version.pdf

42 Joined Cases C-293/12 and C-594/12 Digital Rights Ireland (Judgment of 8 April 2014) ECLI:EU:C:2014:238.

Interception in practice

Surveillance across all of Pakistan's networks is becoming more widespread. Since the creation of the Pakistan Internet Exchange - an communications system that keeps most of Pakistan's communications within Pakistan - the government has been able to route the majority of Pakistan's internet traffic through a single core backbone with limited gateways, making it much easier to monitor internet traffic. Voice over Internet Protocol (VoIP) communications, including popular services such as Skype and Viber, are also heavily monitored. According to an industry source, since at least 2008, the Pakistan Telecommunications Authority (PTA) has required internet service providers (ISPs) to submit their information about their clients in the form of graphs of traffic for each link, along with IP addresses of viewers, ISPs are also required to mention if the specific client is a call center or a client authorized to use VoIP.

Spaces to communicate privately online are narrowing. In 2011, the PTA ordered all ISPs and phone companies to ban encryption and virtual private networks (VPNs) as an anti-terrorism measure. Encryption and VPNs are commonly used to access censored content and maintain communications confidentiality.[43] Banning their use damages the ability of, for instance, journalists and sources to securely communicate information in the public interest.

As part of PTA licensing requirements, service providers must make their networks 'lawful interception-compliant'. There are several ways a service provider can achieve such compliance. They can physically install on their network components that comply with various international interception protocols or, alternatively, they can install external 'probes' somewhere along the transmission cables to allow signals carried on their network to be transmitted to monitoring facilities of requesting government agencies. Government authorities can also install high-powered probes without the knowledge or assistance of providers and gain access to the same data.

Pakistan has a thriving communications surveillance industry that has developed to meet the growing demand for increased levels of surveillance. Pakistani companies such as the Center for Advanced Research in Engineering and the National Radio Telecommunication Corporation of Pakistan have all developed network surveillance tools, partly in collaboration with the military. Other companies provide both interception technologies as well as facilities to monitor and analyse transmitted data.[44]

A wide array of foreign companies provide interception equipment to Pakistani networks. The table details a selection of foreign companies and their clients, based on information from interviews with industry experts and analysis of employee profiles.

43 "Securing Safe Spaces Online: Encryption, online anonymity, and human rights," Privacy International, June 2015, https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_2.pdf

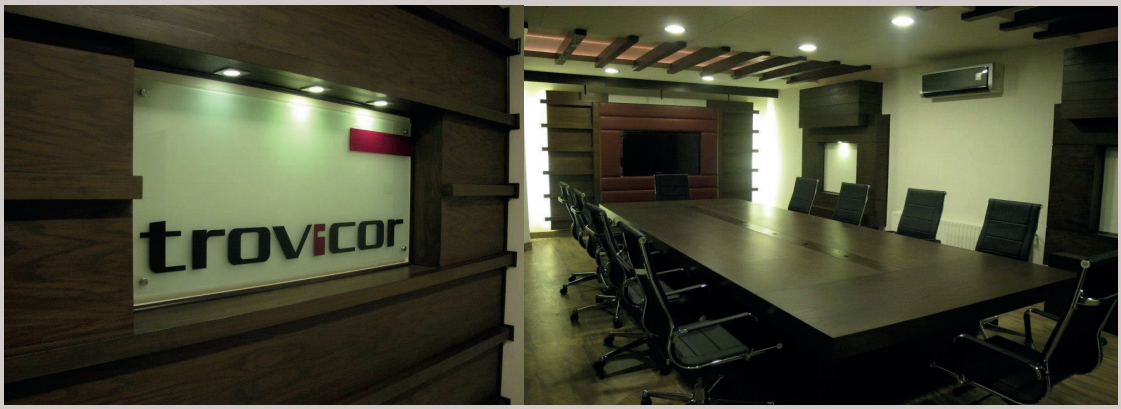
44 Companies sell intercepting technologies, such as interception protocol compliant- mobile switching centres, to service providers and government actors. However, monitoring centres – to which the intercepting technologies transmit data and where analysts treat and analyse the data – are typically sold only to law enforcement and intelligence agencies.

COMPANYHEADQUARTERS)	CLIENT	SOLUTIONS PROVIDED
Alcatel (France)	Unknown clients	Provices Lawful Interception Gateways (LIG) in Pakistan networks since at least 2005
	Pakistan Telecommunications Ltd (PTCL)	Provides a monitoring centre that was integrated with Siemens' Lawful Interception Operating System (LIOS) solution since at least 2009
Atis (Germany)	Unknown security agency	Monitoring centre linked to Pktel, Instaphone and Ufone networks
Ericsson (Sweden)	Warid Telecom	Integrated Utimaco's Lawful Interception Management System (LIMS) solution
Huawei (China)	Mobilink	Provided Lawful Interception Gateways (LIG) to connect with unknown security agency monitoring centres at least since 2006
	Ufone	Provided Lawful Interception Gateways (LIG) to connect to monitoring centres since at least 2006
	China Mobile Pakistan (CMPak)	Tested and installed a Lawful Interception system
Nokia Siemens Networks (NSN) / Trovicor	Ufone	Provided a voice and GPS interception system.
	Telenor	Provided lawful interception capacity since at least 2008
	Mobilink	Provided Lawful Interception Gateways (LIG) since at least 2010.
	Pakistan Telecommunications Limited (PTCL)	Provided Siemens' Lawful Interception Operating System (LIOS) solution that mediates between monitoring centres and service provider networks
SS8	Ufone	Provided Lawful Interception nodes
Utimaco	Wateen Telecom	Provided interception platforms since at least 2007
	Mobilink	Between 2007 and 2010, Utimaco provided a Lawful Interception Gateway (LIG) solution to Mobilink and software to the Islamabad monitoring centre
	Siemens Pakistan	Sold an Interception Management Solution to Siemens Pakistan to be implemented in Telenor Pakistan's networks

Two companies in particular – Trovicor, a German surveillance technology company and the company of which it was formerly a unit, Nokia Siemens Networks (NSN) – were particularly active in providing monitoring centre solutions to the Pakistani government. NSN[45] has been a main player in the Pakistani surveillance market since the late 1990s and was one of the first companies to provide mobile (GSM) network lawful interception capacity in Pakistan.

NSN was a Helsinki-based joint venture of German conglomerate Siemens AG and Finnish telecommunications company Nokia. Following controversy in 2009 when it was revealed that NSN had sold monitoring centre equipment in Iran,[46] NSN sold its subsection, 'Siemens Intelligence Solutions' to Perusa Partners Fund 1 LP, a private investment firm based in Munich, who renamed it Trovicor.[47]

Trovicor continues NSN's legacy. It has expanded the capabilities of various monitoring centres across the world, including those connected to key service providers such as Telenor, Mobilink and Warid. In 2009, Trovicor registered a subsidiary in Islamabad, Trovicor Smc Pvt Ltd.[48] Other Trovicor companies, including Trovicor S.R.O. (Czech Republic),[49] Trovicor D.O.O (Hungary) and Trovicor Solutions FZ-LLC (United Arab Emirates), shipped monitoring centre equipment to Pakistani clients throughout 2014.[50]



CAPTION: Trovicor's Pakistan affiliate has an office in Islamabad.
Credit: Hassan Interiors (2012)

Publicly, NSN distances itself from Trovicor. It maintains that its monitoring centre deals are a thing of the past since 2009. However, in previously unreleased internal memos that stance is not entirely accurate. Guidance provided to NSN employees in 2011 counselled them to respond when questioned: "No we do not sell monitoring centres anywhere around the world. This is a business we exited almost two years ago (March 2009)." (See annex 1, 'NSN Internal Q&A document, 2013') NSN encouraged staff to cite NSN's human rights concerns as the reason for exiting the monitoring centre business.

45 The acronym 'NSN' now commonly refers to 'Nokia Solutions and Networks', instead of 'Nokia Siemens Networks'. The term NSN in this report refers to 'Nokia Siemens Networks.'

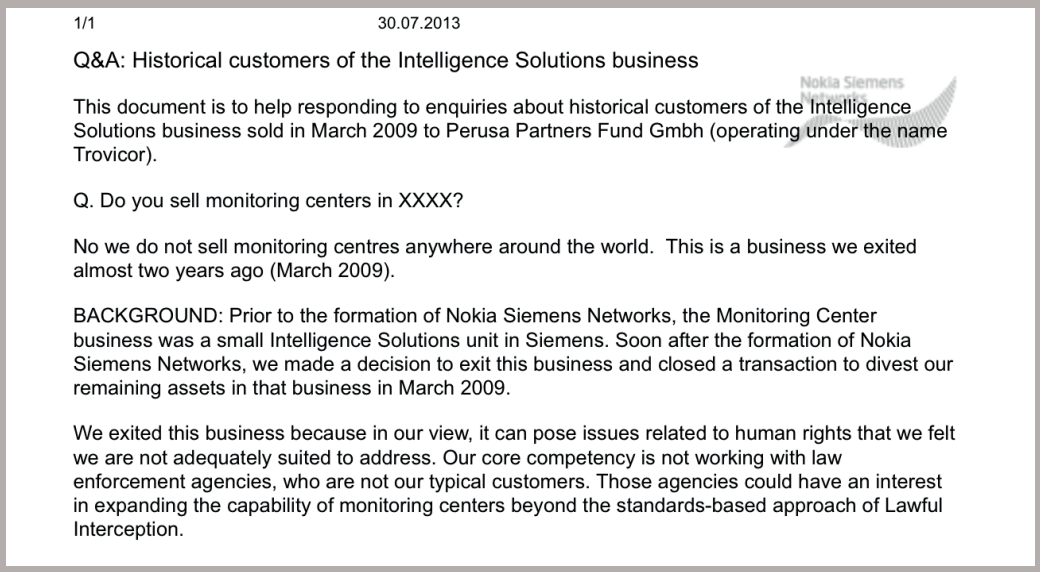
46 "Iran's Web Spying Aided By Western Technology", The Wall Street Journal, 22 June 2009, http://online.wsj.com/news/articles/SB124562668777335653?mg=reno64-wsj&url=http%3A%2F%2Fonline.wsj.com%2Farticle%2FSB124562668777335653.html

47 "Trovicor", Perusa, 24 April 2009, http://www.perusa-partners.de/deutsch/beteiligungen/liste/trovicor.php and "Provision of Lawful Intercept capability in Iran", Nokia, 22 June 2009, http://networks.nokia.com/news-events/press-room/press-releases/provision-of-lawful-intercept-capability-in-iran

48 "TROVICOR (SMC-PVT.) LIMITED", Securities and Exchange Commission of Pakistan, accessed 16 June 2015, http://www.secp.gov.pk/ns/company.asp?COMPANY_CODE=0068909&id=

49 "Trovicor Smc Pvt Ltd", Great Export Import, accessed 16 June 2015, http://en.52wmb.com/b-trovicor_smc_pvt_ltd/7285910

50 "Trovicor", Pakistan Trade Info, accessed 16 June 2015, http://paktradeinfo.com/international-trade-se/trovicor



1/1 30.07.2013

Q&A: Historical customers of the Intelligence Solutions business

This document is to help responding to enquiries about historical customers of the Intelligence Solutions business sold in March 2009 to Perusa Partners Fund Gmbh (operating under the name Trovicor).

Q. Do you sell monitoring centers in XXXX?

No we do not sell monitoring centres anywhere around the world. This is a business we exited almost two years ago (March 2009).

BACKGROUND: Prior to the formation of Nokia Siemens Networks, the Monitoring Center business was a small Intelligence Solutions unit in Siemens. Soon after the formation of Nokia Siemens Networks, we made a decision to exit this business and closed a transaction to divest our remaining assets in that business in March 2009.

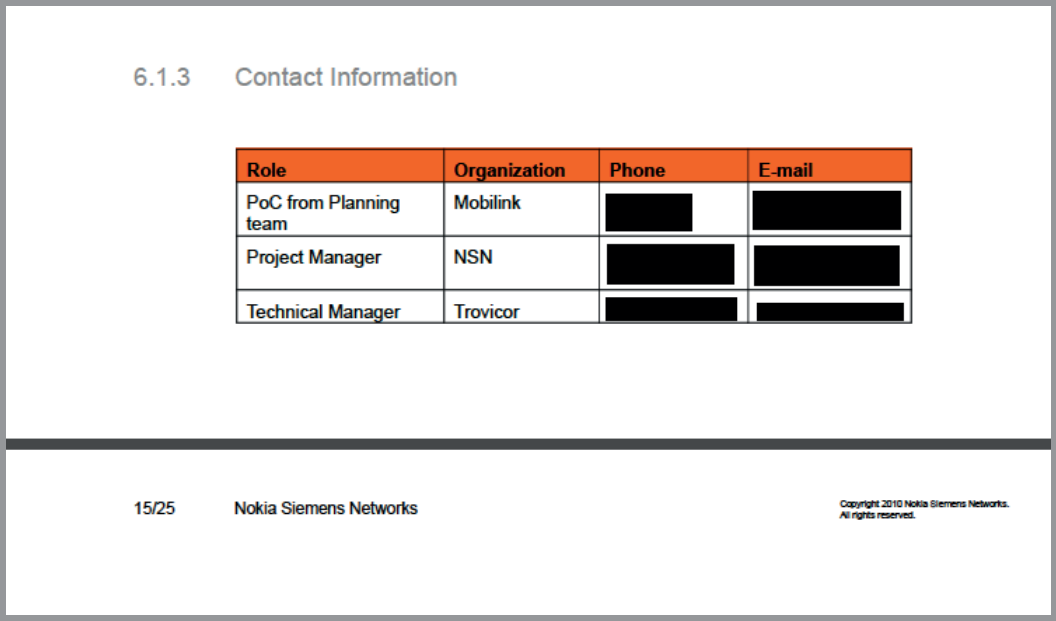
We exited this business because in our view, it can pose issues related to human rights that we felt we are not adequately suited to address. Our core competency is not working with law enforcement agencies, who are not our typical customers. Those agencies could have an interest in expanding the capability of monitoring centers beyond the standards-based approach of Lawful Interception.

CAPTION: NSN encouraged staff, when questioned on NSN's monitoring centre business, that NSN exited the business over human rights concerns.

NSN also maintained that it had "no ownership interest, no operational control, and no role in the management of Trovicor. Neither do we provide support to any of its products." Carefully-worded denials aside, NSN nevertheless cooperated closely with Trovicor to execute at least one monitoring centre project in Pakistan after the break-off. In internal documents that surfaced during the investigation by Privacy International, NSN refers to Trovicor as, alternately, an "NSN vendor"and as a "3rd party who will be delivering the onshore services on behalf of NSN in a 2010-2011 joint project to expand Pakistan's interception capabilities (see annex 2: NSN Project Management Plan, 2010). NSN and Trovicor, working together, expanded the existing Lawful Interception Management System (LIMS) solution provided by Utimaco, a German surveillance company that also often works in close partnership with NSN, to Mobilink, a major Pakistani network. Utimaco, another Germany company that operates in the monitoring centre market, has been selling monitoring centres in Pakistan since at least July 2004. Utimaco sold an Interception Management Solution to Siemens Pakistan to be implemented in Telenor Pakistan's networks, in the amount of over € 500,000 over the period July 2004-May 2005, according to documents seen by Privacy International.

The LIMS is a mediation platform between telecommunications companies and law enforcement monitoring centres. Trovicor was responsible for upgrading the LIMS software, integrating it with the existing mobile switching centres (MSCs), integrating Utimaco's software, testing the system and, crucially, integrating the existing LIMS with the monitoring centre in Islamabad, activities that NSN noted would be handled "by Trovicor independently." Trovicor would ensure integration with Mobilink's existing MSCs, provided by Huawei.

Technically, NSN can claim that it does not support Trovicor's monitoring centre business. But in practice, it continues to work with Trovicor to expand widespread mass communications surveillance capacities across at least one of Pakistan's most important nationwide service providers.



6.1.3 Contact Information

Role	Organization	Phone	E-mail
PoC from Planning team	Mobilink	[redacted]	[redacted]
Project Manager	NSN	[redacted]	[redacted]
Technical Manager	Trovicor	[redacted]	[redacted]

15/25 Nokia Siemens Networks

CAPTION: An NSN employee appears as the overall CSI Project manager "responsible for the delivery of the overall customer project", managing project budgets and management plan. Trovicor was responsible for preparing configurations for the LIMS, resolving any technical issues. NSN and Trovicor appear jointly responsible in project plans. SOURCE: Annex 2: NSN Project Management Plan, 2010

Centralized surveillance of network traffic

The Pakistani government has been trying for years to capture all domestic phone and internet traffic across the nation's networks. As of 2013, they are significantly closer to achieving this goal.

In June 2013, the Inter-Services Intelligence (ISI), Pakistan's best known intelligence agency, sought to develop a mass surveillance system by directly tapping the main fibre optic cables entering Pakistan that carried most of the nation's network communication data. The confidential request for proposals outlines a "Targeted IP Monitoring System and COE [Common Operations Environments]" that aimed to capture and store approximately 660 gigabits of internet protocol (IP) traffic per second under ISI control (See annex 3: 'Inter-Services Intelligence Proposal, 2013'). This system would make available virtually all of the nation's domestic and international communications data for scrutiny, the most significant expansion of the government's capacity to conduct mass surveillance to date.

The total intake of data every second sought by Pakistan in the proposal document would rival some of the world's most powerful surveillance programmes, including the UK's 'Tempora' and US' 'Upstream' programmes.[51] What the ISI wanted to build, according to the request for proposals, was a complete surveillance system that would capture mobile communications data, including Wi-Fi, all broadband internet traffic, and any data transmitted over 3G. According to the documents, the interception activities were to be "seamless" and "must not be detectable or visible to the subscriber".

The total capacity of the actual system, however, could be considerably less and reflect the practical limitations entailed in such an expansion. Only a relatively small number of analyst positions – 200 – were required to operate the system, and the ISI specified in its request that the system be "capable of monitoring 1000-5000 concurrent targets", a small number considering the country's population and use of communication technologies. Yet the programme could be expanded simply with the addition of desks and interfaces to the monitoring centre.

In the first phase of the project, the successful company would provide a centralized command centre (Fusion Centre) capable of receiving a range of data types from mobile and ISP providers. In the second phase, the successful company's 'solution' would need to capture "all international IP (internet protocol) traffic at present," from what is currently five sites. Specifically, from three landing sites for international fibre optic cables and from two satellite data aggregation sites.

The ISI sought to collect subscriber information from the vast majority of service providers ("60 x ISPs/Broadband operators"). Comparing this subscriber data with IP addresses would allow the intelligence service to accurately identify users accessing internet sites and generating IP-based communications traffic. The data intercepted would include alarmingly specific data about the average Pakistani citizen.

ISI also required the successful company to provide "intelligent analysis" in its system. Using voice and pattern recognition tools and open source analysis of social networks, analysts would be required, according to the proposal request, to collate this data with communications data, in order to identify persons of interest, as well as significant levels of personal information about them, all without accessing communications content.

51 Total intake at the required landing sites would be 450 gbps (3 x 150 gbps = 450 gbps for landing sites). Additionally, the system specified that domestic IP traffic be captured at 11-14 points of presence (POP) with a rate of 20-30 gbps.

The ISI's surveillance expansion plan does suggest that the agency was conscious to follow some standard lawful interception procedures, however. Data collected would need to be "divisible into individual components;...the metadata included in the Interception Related Information (IRI) should be separable from Communication Content (CC)" – suggesting that communication content may receive different treatment to metadata.

Yet the dichotomy drawn by various spy agencies between communications content and metadata is a false one. Given that metadata can include the time and location of a communication, its sender and receiver, and the subject line of a communication, metadata still reveals a striking amount of personal data, which can be used with other methods to further violate an individual's privacy. The system sought was also to log all lawful interception-related activities and exhorts that "sensitive data must be protected during transmission and the privacy of an individual's records and personal information should be safeguarded." Yet with potentially all traffic in and out of Pakistan, of citizens and non-citizens alike being captured, individuals' privacy rights would already have been invaded, with the risk of abuse, and further human rights violations, is very real.

Packet inspection

The same technologies that the Pakistani government uses for censorship are also used for surveillance. Censorship of online content is widespread and justified as a means to prevent the sharing of pornographic, obscene, and blasphemous material in the Islamic republic.[52]

To this end, the Pakistani government has purchased a number of 'packet inspection' technologies, some of which are profiled below. Packet inspection technologies examine the constituent pieces of data that make up internet and communications traffic as they pass inspection points in the internet architecture, searching for signatures that the technologies recognize as abnormal, such as viruses and spam. Packet inspection technologies can also be programmed to search for particular terms, such as key words in emails.

From 2007 until at least 2010, the PTA had a working relationship with the American company Narus.[53] Narus sells an internet monitoring product called NarusInsight that passively monitors information packets as they travel through the network, running them against control lists provided by the operator of the product or by law enforcement.

Pakistan Telecommunications Ltd (PTCL), Pakistan's largest telecommunications company, which also operates the Pakistan Internet Exchange, has proxies in place to do "deep packet inspection" of internet traffic. The technology to conduct deep pack inspection were provided, in part, by US-based Blue Coat systems, according to industry sources. Blue Coat's "ProxySG" product acts as a gatekeeper of access to the internet and services within it, from Secure Socket Layer (SSL) encryption, to HTTPS. Packet filtering products by Netsweeper have also been installed on Pakistan Telecommunication Company Limited (PTCL)'s network, according to a 2013 investigation by The Citizen Lab[54] and have been a vital tool in the government's censorship of the internet.

52 "Pakistan's Internet Landscape", Bytes for All Pakistan, November 2013, http://content.bytesforall.pk/sites/default/files/MappingReportFinal%20-%20Published.pdf

53 "PTA to Acquire Technical Solution for Illegal Telecom Traffic",Pakistan Telecommunications Authority (PTA), 9 October 2007, http://pta.gov.pk/index.php?option=com_content&view=article&id=1008:pta-to-acquire-technical-solution-for-illegal-telecom-traffic&catid=92:press-releases

54 "O Pakistan, We Stand on Guard for Thee: An Analysis of Canada-based Netsweeper's Role in Pakistan's Censorship Regime", The Citizen Lab, 20 June 2013, https://citizenlab.org/2013/06/o-pakistan/

Tactical surveillance

Pakistani law enforcement and intelligence agencies also use a number of different tactical communications surveillance technologies. Tactical interception technologies are surveillance tools that collect intercepted communications data either wirelessly or directly from a target device rather than from the service provider's network architecture. They can be easily transported to different locations for deployment. Such equipment includes IMSI Catchers. IMSI Catchers are monitoring devices that transmit a strong wireless signal, which work to entice nearby phones to connect to the IMSI catcher, rather than mobile phone towers, as they normally do. These devices are capable of being 'targeted' at a particular individual's device by, for example, being aimed at his or her workplace. Yet they can also be used to identify unknown persons attending demonstrations and other gatherings because as many mobile phones as the system can accommodate will connect to the IMSI catcher and transmit it information about the mobile phone user, including the location of a target to within one metre.

Mobile monitoring equipment for identification and/or interception is particularly widely used by law enforcement agencies across Pakistan.[55] The Pakistani government has imported many of these tactical communications surveillance technologies from Europe. In 2010, Germany granted German companies export licenses valued at € 3.9 million to export "monitoring technology and spyware software"[56] to Pakistan. Between 2012 and 2014, Swiss companies were granted licenses to export dual-use communications surveillance technology to Pakistan.[57] The total value of the three exports based on the category provided was over CHF 1 million according to records obtained by Privacy International.[58] Finland, too, granted licenses to companies based in Finland, exporting surveillance technologies to Pakistan. For instance, the Finnish export authority authorized four export licenses to ABB, a Finnish automation technology company, to provide "waveform digitisers and transient recorders" in Pakistan, which are used to analyse audio and remote sensing data.

The Pakistani government is also a confirmed user of intrusion technologies which enable the remote hacking of targeted devices. Intrusion technologies are capable of collecting, modifying and extracting all data communicated and stored on a device. To do this, malware, short for malicious software, must be installed on the device. Installation often occurs when the user inadvertently installs a trojan, which is a disguised or concealed programme. Once the trojan is installed it embeds itself in all system functions, collecting and transmitting data to the operator of the trojan as the infected device operates normally from the user's perspective. Malware provides its operator with extraordinary access to an individual target's computer. They can view an individual's actions in real time on their computer, enabling the user to records passwords, and even impersonate the target; sending out e-mails and Facebook messages as the target, for example. The user can also use the trojan to turn on the camera and microphone on a target's computer, thereby seeing and hearing everything in the vicinity of the target's computer, without the target ever being aware. Due to their staggering monitoring capabilities, intrusion technologies are eagerly sought , bought and used by repressive regimes worldwide.

55 For example, in 2014, the Sindh police forces reportedly acquired a Caller Location Identification System (CLIS) that they had been trying to acquire since 2010. The Punjab police also acquired IMSI/IMEI and location tracking technology in 2015. See "CID gets mobile phone caller locator system", DAWN, 13 October 2014, http://www.dawn.com/news/1137548/cid-gets-mobile-phone-caller-locator-system and "Punjab police to have mobile phone tracking units", NewsLens Pakistan, 8 June 2015, http://newslens.pk/punjab-police-mobile-phone-tracking-units/

56 "Überwachungstechnologie und Späh- software"

57 These licenses correspond to the 5A001f category of dual-use goods controlled by the Wassenaar Arrangement. This category covers "mobile telecommunications interception or jamming equipment", including interception equipment for " extraction of voice or data" or " extraction of client device or subscriber identifiers". "Dual-Use List – Category 5 – Part 1 – Telecommunications", Wassenaar Arrangement, 25 March 2015, http://www.wassenaar.org/controllists/2014/WA-LIST%20%2814%29%202/07%20-%20WA-LIST%20%2814%29%202%20-%20Cat%205P1.doc

58 The total value of the exports of 5A001f equipment to Pakistan from Switzerland between 2012 and 2014 was CHF 1,059,527. This occurred in three separate shipments in June 2012 (CHF 5,500), October 2013 (CHF 538,025) and June 2014 (CHF 516,002).

In April 2013, computer forensic research by The Citizen Lab revealed the existence of a command and control server for FinFisher, an intrusion malware suite, operating within Pakistan.[59] FinFisher is an intrusion technology suite produced by German-based company FinFisher GmbH. Prior to 2013, the FinFisher suite was sold by Anglo-German company Gamma International. The following year, documents obtained from a FinFisher server revealed support requests from an apparent Pakistani client – identification number 'ID 32' – dating back to 2011. In 2013, following this revelation, Pakistani civil society group, Bytes for All, filed a petition in the Lahore High Court – the court ordered the PTA to look into the matter and produce a report within one month. The PTA has not filed their report, and attempts to gain further hearings on the issue have been unsuccessful.[60]

Pakistan also sought to acquire intrusion malware from Hacking Team, an Italian company and rival of FinFisher. Pakistani companies attempted to contract business with Hacking Team for sale to Pakistani law enforcement or intelligence clients in March 2015.[61]

59 "For Their Eyes Only: The Commercialization of Digital Spying", The Citizen Lab, 30 April 2013, https://citizenlab.org/2013/04/for-their-eyes-only-2/

60 "Loss of privacy is always permanent - Snags in hearing of FinFisher case at Lahore High Court", Bytes for All Pakistan, 22 August 2014, https://content.bytesforall.pk/node/143

61 "Fwd: Find Business Opportunities in Pakistan", email published by Wikileaks, 2015, https://wikileaks.org/hackingteam/emails/emailid/616153

Conclusion

The practical capacity of the Pakistani government for communications surveillance now outstrips the current capacity of domestic and international law for effective regulation of that surveillance.The ISI, in particular, set out to build a stronger, more centralized communications surveillance architecture, and the evidence suggests that they have been successful in doing so. This has real implications for Pakistani citizens' enjoyment of their human rights, and for Pakistan's democracy more generally.

Pakistan's surveillance capacities have been provided by domestic and foreign surveillance companies, as well as by hybrid public-private research entities. A more rigorous export control regime outside of Pakistan, including in EU countries and other states from which surveillance technology is being sold to Pakistan, would contribute to protecting fundamental human rights in Pakistan. The right to free speech and free association depends in part on the right to privacy – all at risk, when, as in Pakistan, armed conflict and insecurity are increasingly used to justify mass surveillance.

Pakistan's laws need to be updated to come into line with international standards, including the International Convention on Civil and Political Rights. The government must seek reforms in line with statements from international bodies such as the UN Human Rights Committee on the interference with rights via surveillance. It is hoped this report will serve the growing number of voices calling for reform inside and outside the National Assembly in Pakistan.

This report, and the investigation that preceded it, has revealed the continued business by companies who were thought to be have exited the sale of surveillance equipment. It has revealed the intentions of an intelligence agency to create a mass surveillance programme in Pakistan, that races past the domestic legal framework that would underpin it. An investigation into the status of the project should immediately take place, including any assessment of the projects adequacy, legality, necessity and proportionality. The citizens of Pakistan deserve an explanation from the government.

Ultimately this report details the age old issue in communications surveillance: modern capabilities in the hands of powerful agencies underpinned by vague, imprecise, dated laws. The imbalance when these two factors are present risks the loss of hard won freedoms for the individual. The scales need to be tipped towards a balanced system where modern, progressive, transparent laws and processes are in place that hold powerful institutions to account and seek to guarantee the rights of everyone affected by the practices detailed throughout this report.

Annexes

Q&A: Historical customers of the Intelligence Solutions business

This document is to help responding to enquiries about historical customers of the Intelligence Solutions business sold in March 2009 to Perusa Partners Fund Gmbh (operating under the name Trovicor).

Q. Do you sell monitoring centers in XXXX?

No we do not sell monitoring centres anywhere around the world. This is a business we exited almost two years ago (March 2009).

BACKGROUND: Prior to the formation of Nokia Siemens Networks, the Monitoring Center business was a small Intelligence Solutions unit in Siemens. Soon after the formation of Nokia Siemens Networks, we made a decision to exit this business and closed a transaction to divest our remaining assets in that business in March 2009.

We exited this business because in our view, it can pose issues related to human rights that we felt we are not adequately suited to address. Our core competency is not working with law enforcement agencies, who are not our typical customers. Those agencies could have an interest in expanding the capability of monitoring centers beyond the standards-based approach of Lawful Interception.

Q. Did you sell monitoring centers in XXXX?

That part of the business was sold to Perusa Partners fund, and operates under the name Trovicor. We do not provide information on historical deals where the business is no longer part of Nokia Siemens Networks. You will have to address your questions to the current owners of this business. Nokia Siemens Networks has no ownership interest, no operational control, and no role in the management of Trovicor. Neither do we provide support to any of its products.

Q. You talked about the monitoring capability provided to Iran, why is this different?

The disclosure about Iran was initially made before the business was sold in March 2009.

Specific facts about our business in Egypt:

- Our customers in Egypt include Etisalat, Vodafone and Orascom
- We have approximately 400 Employees, mainly located in Cairo and Giza
- By 2 February 2011 we had evacuated 55 people – foreign employees and their families – from Egypt

It is best to avoid getting into a discussion of the Intelligence Solutions business.

However, a supplementary background Q&A provides details on: the existence of lawful interception capabilities in telecommunications networks everywhere, the reasons for us exiting the monitoring center business and how we work to minimize the potential for human rights to be infringed by the technology we sell.

Nokia Siemens Networks

Mobilink
LIMS expansion
Project Management Plan

Table of contents

1. Introduction

The Project Management Plan (PMP) is a formal, approved document that defines how the project is executed, monitored and controlled. This document describes in summary or in details the subsidiary project plans and planning documents. The PMP describes the commitments, requirements, dependencies and risks that exist in the project.

This document is written for the project team and the project sponsors. The purpose is to:

1. Outline the project-goals (scope, timeframe, and budget),
2. Describe the project scope of deliverables for the main stakeholders,
3. Describe the project team members roles and responsibilities
4. Provide a starting point for project audits or compliance reviews
5. Capture the approach to be adopted during the delivery, and
6. Act as a communication vehicle for all stakeholders during the work in progress.

This document applies for all project team members and is valid until the end of the project.

2. Document History

Date	Issue	Author	Approver	Comments

Table 1: Document history

3. Project Overview

This section presents an overview and objectives of the project.

3.1 Background

The existing LIMS server is currently used for Marking Circuit Core subscribers for Mobilink R99 and R4 MSCs from Nokia Siemens Networks. The requested scope is for additional marking capacity and marking capability of Huawei MSC subscribers as step 1. And in second step to completely shift this service and the exiting services on LIMS to the new LIMS hardware.

3.2 Project Description

In existing system, Huawei has its own LIMS and NSN has its own for their respective MSS. Both LIMS systems are end of support and Mobilink has decided to bring in a new LIMS system from NSN to integrate all the MSS and GMSCs on their network. Trovicor is a 3rd party who will be delivering the onshore services on behalf on NSN.

3.3 Solution Architecture

The new LIMS solution if by NSN partner utimaco and it is based on SUN M4000 server machine. The Existing LIMS needs to be upgraded to version 7.4. The communication module for connecting Huawei MSCs needs to be installed for catering marking capability of Huawei MSC subscribers.

3.4 Objectives and Constraints

3.4.1 Objectives

The key project objectives are:
Roll out the new LIMS and integrate all Huawei and NSN MSS existing on Mobilink's network on to it.

3.4.2 Constraints

The key project constraints are:
Huawei LIMS is being swaped here so we do not expect required level of cooperation from Huawei.

4. Project Scope

This section presents the scope of the project.

4.1 In scope

Scope of services and SOR STEP 1:

1. Upgrading the LIMS software level to 7.4. (Trovicor)
2. Upgrading the LIMS system with Communication module for marking capability of Huawei MSCs. (Trovicor)
3. Integration of the upgraded system with the Huawei MSCs. (Trovicor)
4. Acceptance testing and standard ATMN. (Trovicor)
5. Integration of the exiting LIMS with the Monitoring center is not part of this scope. This will be handled by Trovicor independently vial Mobilink.

Scope of services and SOR STEP 2:

1. Installation and commissioning of the new hardware for LIMS (SUN M4000). (Trovicor)
2. - Create a full system backup (Trovicor)
3. - Upgrade the LIMS. (Trovicor)
4. - Migrate Database. (Trovicor)
5. - Connect and configure the LIMS to the existing network elements which are also connected to the current LIMS. (Trovicor)
6. - Update the LIMS with the latest patch set. (Trovicor)
7. - Test the interworking with the connected network elements with both vendors, NSN and Huawei. (Trovicor)
8. - Run basic test cases on the LIMS (creating/deleting targets, IRI-ticket processing) (Trovicor)
9. - Create a full system backup and store basic LIMS configuration settings. (Trovicor)
10. - Execute the acceptance test cases. (Trovicor)
11. - Test the interworking with the connected monitoring center is not part of the requested scope. This will be handled by Trovicor independently vial Mobilink

4.2 Out of scope

- Any other requirement not clearly stated in “in scope” section of this document.

4.3 Deliverables

The following deliverables are within the scope of the project. These are standard deliverables in most cases. Non-standard deliverables, or where there is clarification or extension of the standard, are described in more detail. Deliverables are for NSN and customer use except where shown.

4.3.1 Software/Hardware

- M4000 Server with rack and all other required accessories as mentioned in the BoQ
- Utimaco software along with required licenses

4.3.2 Documents

- Solution description
- Acceptance test documents
- Project plan
- Status reports
- LIMS connectivity diagram

4.3.3 Services

- Installation, Commissioning, integration
- On-site assistance in Customer Acceptance Test
- MSS DB creation and successful testing with Monitoring centers.

4.4 Assumptions

The major assumptions made while preparing this project plan and determining the milestone dates are:

Mobilink is assumed to provide the following:

Power, Space and network connectivity till racks
All configurations on MSS side.
Acceptance test cases approval
Approval of UAT
Site Access
Configurations on Network Entities (routers, switches MSS etc)
Cooling requirement availability.

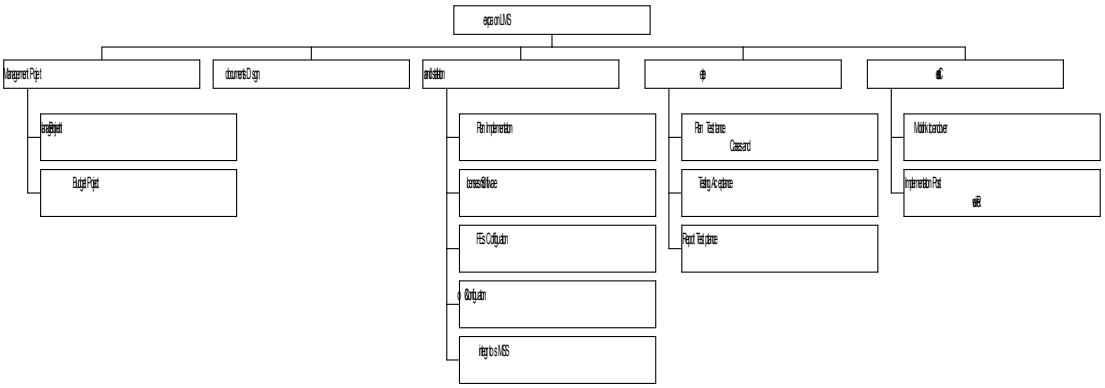
4.5 Dependencies

The major dependencies made while preparing this project plan and determining the milestone dates are:

1. Completion of configurations on MSS by respective vendors.
2. Power, LAN and space as required are available before commissioning work starts.

5. Project Definition

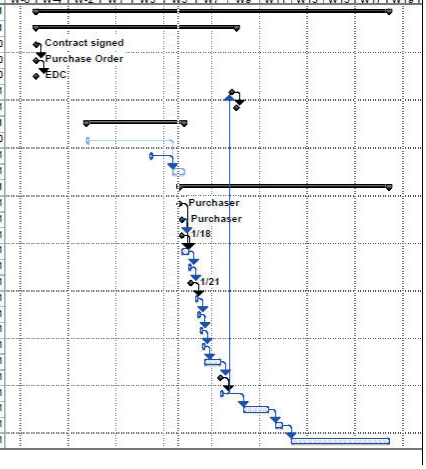
5.1 Work Breakdown



5.2 Schedule Overview/Gantt Chart

NSN (Mobilink) LIMS Upgrade ON-1299
Tentative Project Implementation Plan

ID	Task Name	Duration	Start	Finish
1	**NSN (Mobilink) LIMS Upgrade Services**	**110 days**	**Mon 11/15/10**	**Mon 4/18/11**
2	**Commercial Milestones**	**63 days**	**Mon 11/15/10**	**Thu 2/10/11**
3	Contract signed	0 days	Mon 11/15/10	Mon 11/15/10
4	Purchase Order	0 days	Mon 11/15/10	Mon 11/15/10
5	Effective Date of Contract (EDC)	0 days	Mon 11/15/10	Mon 11/15/10
6	Provisional Acceptance Certificate	0 days	Tue 2/8/11	Tue 2/8/11
7	Invoice on PAC	0 days	Thu 2/10/11	Thu 2/10/11
8	**Project Kick Off / Site Inspection**	**30 days**	**Tue 12/7/10**	**Tue 1/18/11**
9	Project Kick off	1 day	Tue 12/7/10	Tue 12/7/10
10	Site Survey	1 day	Tue 1/4/11	Tue 1/4/11
11	Site Work Completion	3 days	Fri 1/14/11	Tue 1/18/11
12	**Implementation**	**66 days**	**Mon 1/17/11**	**Mon 4/18/11**
13	Site ready for installation	0 days	Mon 1/17/11	Mon 1/17/11
14	HI2/HI3 links to MC available	0 days	Tue 1/18/11	Tue 1/18/11
15	Equipment Delivery on Site	0 days	Tue 1/18/11	Tue 1/18/11
16	Installation LIMS (HW M4000 / SW Ver 6.1)	3 days	Tue 1/18/11	Thu 1/20/11
17	Import of DB from old LIMS V480	1 day	Fri 1/21/11	Fri 1/21/11
18	Delivery of DB from Lahore to Islamabad	0 days	Fri 1/21/11	Fri 1/21/11
19	Import of DB on New LIMS M4000	1 day	Mon 1/24/11	Mon 1/24/11
20	Test of First NSN R4 MSS to verify new LIMS operation	1 day	Tue 1/25/11	Tue 1/25/11
21	Software upgrade of new LIMS M4000 to LIMS Ver 7.6	1 day	Wed 1/26/11	Wed 1/26/11
22	Huawei GMSC Com Module Installation	1 day	Thu 1/27/11	Thu 1/27/11
23	Integration & Testing of Huawei GMSC - Total 3 GMSCs	5 days	Fri 1/28/11	Thu 2/3/11
24	Ready for Operation	0 days	Thu 2/3/11	Thu 2/3/11
25	Acceptance Test	1 day	Fri 2/4/11	Fri 2/4/11
26	Shifting of NSN R4 MSS to new LIMS & Testing - Total 9	9 days	Mon 2/14/11	Thu 2/24/11
27	Shifting of NSN GPRS to New LIMS & Testing	3 days	Mon 2/28/11	Wed 3/2/11
28	Shifting of Huawei MSCs to new LIMS (Total 31)	31 days	Mon 3/7/11	Mon 4/18/11



5.3 Key Milestones / Dependencies

Key Milestone / Dependency	***Date***
Site ready	17th January 2011
Equipment delivered	17th January 2011

RFS	26th January 2011
Acceptance testing completion	04th February 2011
Integration completion	18th April 2011

5.4 Delivery Approach

Project will be managed with a linear approach: Installation->configurations and license upgrade-> integrations-> Testing-> compete integrations

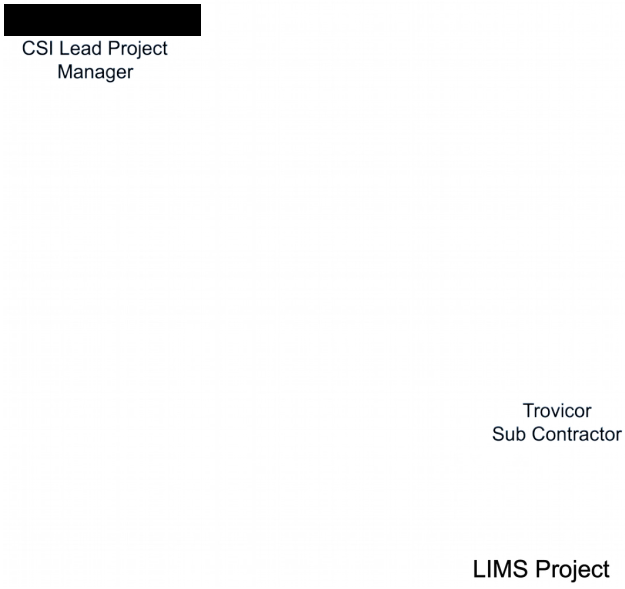
5.5 Critical Paths

H/W delivery-> Site readiness-> Installation and Commissioning
License upgrade-> MSS integrations-> Acceptance testing

6. Project Resources

6.1 Human Resources

6.1.1 Project Organization Chart



6.1.2 Roles and Responsibilities

In this section the project roles and responsibilities are identified, as well as sharing of responsibilities between NSN CSI and the customer. A project team of specific CSI resources will be established under the NSN CSI Project Manager.

6.1.2.1 Responsibilities Table

The following table shows responsibility for the various tasks. Other resources may be required for the delivery of the tasks, but for each there is only one responsible person.

Role	Responsibility
NSN CSI Project Manager	Responsible for the delivery of the overall customer project to meet its committed timescales. Responsible for risk and issue management. Responsible for cost management. Project Management Plan Project Budget Gantt chart
Mobilink Project Manager	Responsible for resolving customer issues. Responsible for ensuring timely site and network access. Responsible for acceptance and all the activities as finalized in the

Role	Responsibility
	Share of responsibility document.
Trovicor- NSN vendor for delivery of this project.	• Solution Detailing • Interfaces Specification • Resolving any technical issues on the project. • Preparation of configurations • Preparation of ATP • Responsible for implementation of configurations and resolve on site issues. • Responsible for running ATPs with customer

6.1.2.2 Share of Responsibilities between NSN CSI and Customer

R	Responsibility	
S	Support	
X	Not responsible	
	NSN/ Trovicor	Mobilink
Equipment ordering and handover to ML's Freight forwarder	R	X
Site readiness	X	R
H/W installation	R	X
Connectivity with IPBB	X	R
Software installation	R	S
DB back up and restoration	R	S
MSS integration	R	S
MSS DB creation at LIMS end	R	X
MSS configurations for integration with LIMS	X	R
Acceptance testing	R	S
ATP sign off	S	R
Handover to ML's support team	R	S

6.1.3 Contact Information

Role	Organization	Phone	E-mail
PoC from Planning team	Mobilink	[redacted]	[redacted]
Project Manager	NSN	[redacted]	[redacted]
Technical Manager	Trovicor	[redacted]	[redacted]

Role	Organization	Phone	E-mail
		[redacted]	[redacted]

6.2 Non Human Resources (Infrastructure)

6.2.1 Implementation and Test Environments

N/A

7. Risk Management

In this section the key risks are identified. A separate risk register will be maintained by the project manager to track risk management.

7.1 Key Risks Identified

	Title	Description	Mitigation Action	Owner
1	Delay in H/W delivery	Delays in getting H/W on site	Close coordination with NSN and ML logistics team	PM
2	Site not ready in power, space and connectivity	Power and network connectivity is not available before the H/W commissioning starts	Relevant requirements to be communicated to customer in time and close coordination with customer in getting any open issued closed as per the PIP	PM
3	Software/ licenses availability	Any delays from Utimaco	Daily follow up and ensuring that all required information is available well in time	PM
4	Commission and installation issues	Issues faced during commission and installation	MOPs finalzed and verified by the Trovicor team before the I&C work is to start.	Trovicor
5	Resource unavailability/ competence issues	Required resources not available for project	Vendor is being asked to introduce their team with NSN PM and ensure availability fo resources	PM
7	H/W issues	Equipment delivered is not complete as per requirements for project delivery	BoQ to be verified by project experts as well Trovicor	PM
8	Site issues	Any permissions/ information/ resource required to deliver onsite activities	During internal project kick off, all such requirement should be gathered from leads/ engineers on site	PM
9	Share of responsibility between NSN and Mobilink	Either parties assuming the other side would do a particular activity.	Finalization of share of responsibilities with customer.	PM

11	Integrational issues/ issue with product	Any particular issue faced from the product during integrational activities.	Alignment with Utimaco technical support before project starts.	PM
12	Financial issues	Any unforeseen activity which was not considered at the time of costing.	Certain budget should be approved as risk buffer.	PM
13	Law and order situation/ unplanned public holidays	Law and order situation at concerned site can cause delays in the project.	Understanding with customer that such delays will be added to PIP without any penalties to either parties.	PM

7.2 Risk Management Process

In order to efficiently identify and manage risks, the project applies the following Project Risk Management process as defined in the NSN CSI Risk Management Policy:

- Identify Risks: This is the process of determining which risks may affect the project and documenting their characteristics.
- Perform Qualitative Risk Analysis: This is the process of prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact.
- Plan Risk Responses: This is the process of developing options and actions to enhance opportunities and to reduce threats to project objectives.
- Monitor and Control Risks: This is the process of implementing risk response plans, tracking identified risks, monitoring residual risks, identifying new risks, and evaluating risk process effectiveness throughout the project.

As input on risk management processes the following data sources may be used:

- Expert Knowledge,
- Analogous Estimation,
- Performance Reports, and
- Stakeholder Information.

The overall Risk Management is illustrated below:

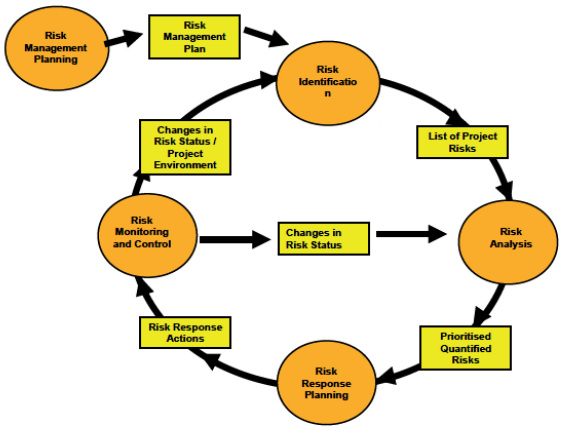


Figure n: Risk Management Process

8. Change (Scope) Management

Changes in the project scope must be issued via a Change Request (CR) Form. The changes will be accepted/denied by the Change Control Board composed by < list the CCB members >. The figure below illustrates the Change (Scope) Management process.

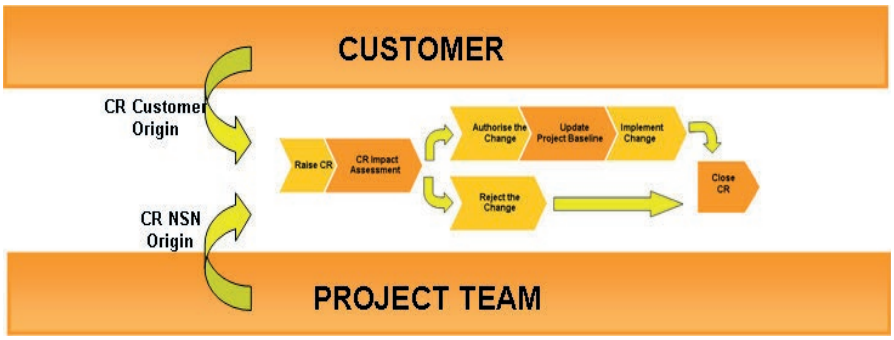


Figure n: Change (Scope) Management Process

9. Project Communication

9.1 Reporting

9.1.1 Customer Project Reporting

The Project Manager will prepare a regular project report to the customer and other stakeholders as agreed. The report will summarise progress since the last report, current activity, and activity due to start within the next period. The report will describe the current risks and issues that are visible to the customer. It will also list the baseline milestones and latest dates. The frequency of the report will be agreed with the customer.

9.1.2 Reporting Plan

Report	Content	Frequency	Reporting (From – To)
Weekly status report	**Status update, upcoming tasks, variances if any, issue and risks**	**weekly**	**PM->CT->Customer**

9.2 Project Progress Reviews

The Project Manager will arrange regular reviews of progress with the project team to confirm the status of all activities that are underway, or about to start. The Project Manager will update the estimates to complete, and timescales based on this meeting, and produce a project progress report minuting the key points of the discussion, and the latest dates. The frequency of meetings will depend on the size of project. Ideally meetings will coincide with phase ends.

Review Type	Attendees	Periodicity	Agenda
Bi Monthly status meetings	PM NSN, POC planning team ML, Technical Manager Trovicor	Bi Monthly	**Project status and issues**

9.3 Escalation Path

Problem Type	First Level of Escalation	Second Level of Escalation
Management/ Technical	**Account Manager**	**CT head**

9.4 Document Management

All documents will be updated on sharenet.

10. Quality Management

Every aspect in triple constraints serves as a parameter to define the success of the Project. Quality indicates the extent to which the final deliverables meet the customer requirement. To ensure that the Project meets the requirement of the Customer, quality of the deliverables produced will be continuously measured along with the management processes used for producing the deliverables.

10.1 Quality Control

Quality control plan serves as an internal mechanism to ensure the deliverables are matching the quality established. Following techniques would be used to perform the quality control:

Peer Reviews: Planned activity where one Project Manager would be evaluating the work being done by other Project Manager. This would allow disclosing any quality issue early during the execution.

Deliverables Review: Review of all the documentations and other deliverables will be planned to ensure the quality. After review a review record is submitted to the project manager for further reporting and archiving.

Phase Reviews: If the project is being executed in multiple phases, there will be review conducted after each phase to determine whether the Project has met the defined goals so far.

Activities/ Techniques	Work Products	Description	Frequency
<<One of the technique listed above>>	<<Produced items to pass through the activity>>	<<Description of the technique being used>>	<<Frequency of each technique to be determined>>

10.2 Lessons Learnt Plan

The section will be updated before project closure.

10.3 Customer Satisfaction KPI

Customer Satisfaction will be measured based on the results of the CSI Project Satisfaction Survey Questionnaire following the process described in the CSI Project Satisfaction Survey Policy.

Survey no.	When (dd/mm/yy)	Customer Stakeholders to be Interviewed

11. References

12. Glossary

Abbreviation	Definition
CAT	Customer Acceptance Test Plan
CCB	Change Control Board
PMP	Project Management Plan
WBS	Work Breakdown Structure
PM	Project Manager
TM	Technical manager
CT	Customer team

CONFIDENTIAL

DIRECTORATE GENERAL
INTER SERVICES INTELLIGENCE
ISLAMABAD

Subject: **Provision of Tech and Financial Proposal**

You are requested to provide subject proposals of IP LI system developed by your company in the light of attached GSR (anx A). Feasibility alongwith technical and commercial proposals may be submitted by 29th June 2013 to this office for evaluation / necessary perusal, please.

For CCO
(Muhammad Tahir Ch)

[redacted]

No [redacted]/51/Sec-701 dated 18 June 2013

CONFIDENTIAL

GSR FOR TARGETED IP MONITORING SYSTEM AND COE

1. Targeted IP monitoring system should cater for at-least following broad Requirements. If there are any additional features in the proposed solution the same may also be highlighted separately:-

Phase-1

a. **Common Operations Environments (COE)**. The proposed IP monitoring solution should cater for all inputs through API's to be integrated in a central command center (One Master MC) thus forming a common operation Picture (COP) within the Fusion Centre. The COE will cater for inputs from following technologies/Platform:-

(1) GSM, 3G / GPRS, LTE

(2) CDMA

(3) Wi-Max

(4) ISP's ,Mega POPs and 3 x IGW's (for Radius and Content Info Gathering)

(5) Provision of GSM / IP data user location system for integration especially 3G compliant.

Phase-2

b. All international IP traffic at present (150Gbps) at 3 landing and 2 x Satellite IPLCs sites with expandability options is required to be monitored.

c. Domestic IP traffic is required to be captured at 11-14 POP with approx aggregated traffic of 20-30 GBps each.

d. Radius information of subscribers is required to be intercepted at approx 60 x ISPs/Broadband operators for co-relation of IP address with subscriber identity.

e. The system should be scalable and modular to meet future requirements/expansion plan of operators.

f. The supplying vendor must provide in writing that the company will open its interfaces (API's), if asked by the buyer to any third party for system/services Integration / analysis.

g. The monitoring system should cater for following:-

(1) Targeted coverage of entire IP traffic, through IP address, subscriber ID, MAC ID or string search, etc.

(2) Content retention/storage of targeted traffic for 90 days.

(3) A Monitoring Centre with a disaster recovery site.

(4) Fifty (50) analyst positions for IP only in Phase-1 and another 150 positions in Phase-2 for Voice.

(5) Provision of intelligent analysis (on IPDR) e.g. link chart analysis, voice/pattern recognition, social networking trends etc.

(6) Provision of indexing and searching stored contents through application of filters.

(7) Capable of monitoring 1000 - 5000 concurrent targets.

(8) The proposed LI system should be capable to be shared with multiple LEAs if desired by this agency.

(9) Able to map / translate IP address of target to its real ID (Collected from RADIUS Servers).

(10) Provision of location IP data user for targeted IP traffic especially 3G compliant.

(11) Support for IPv6, 2G/3G/4G Packet Switch and Circuit Switch or combination of both technologies and IP Networking technologies .Presently in 2G technology regime, the system should cover all GPRS/EDGE traffic originating from Mobile operators.

(12) Capable of intercepting / decoding selected https / encrypted IP traffic in various protocols.

2. The system should be at least(but not limited to) have following capabilities

a. The LI solution must be able to intercept all applicable communications of a certain target without any gaps in coverage.

b. The system should have capability to intercept seamless traffic from network without posing any quality degradation and delays-jitter to the passing traffic.

c. Intercepted communications data should be divisible into individual components; for example, the metadata included in the Interception Related Information (IRI) should be separable from the Communication Content (CC).

d. The monitoring activities performed by the solution must not be detectable or visible to the subscriber.

e. Following a request for lawful interception, a solution must be able to provide real-time response in delivering intercepted data.

f. The solution must have adequate capacity to handle the scope and scale of requested interception.

g. Sensitive data must be protected during transmission and the privacy of an individual's records and personal information should be safeguarded. Only authorized personnel should be able to view intercepted data.

h. Encrypted data shall be delivered in plain text format if the encryption keys are available to the service provider or network operator, for easy integration with other systems.

i. All LI-related activities must be recorded and logged as part of a centralized record-keeping procedure.

j. Flexible interfaces with either Internal Interception Functions (vendor equipment internal interception functions – IIF) or External Interception Functions (Probes – EIF).

k. Secure and encrypted interfaces between the Network Components and the LEA monitoring facilities.

l. The system should at least(but not limited to) support following encryption schemes for data transmissions and delivery

(1) AES
(2) IPsec
(3) TLS
(4) SSH
(5) DES

m. The system should be able to perform Consistency Checks to :-

(1) Prevents malicious human intervention, and human or technical errors.

(2) Guarantees coherence between the data in the network internal interception functions and the interception specifications in system's database. Consistency checks can occur on a regular or random basis, manually and/or automatically.

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422v 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471