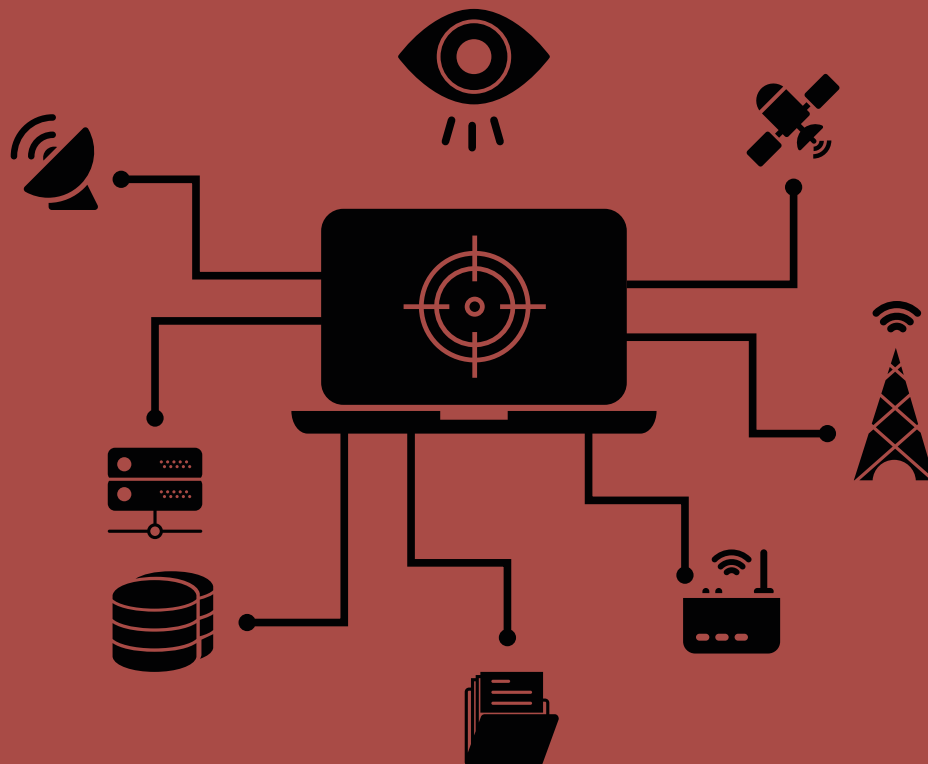


OPEN SEASON

Building Syria's Surveillance State



Acknowledgements

Privacy International acknowledges the many individuals and organisations with whom we spoke who cannot be named.

This report is primarily based on original documentation provided in confidence to Privacy International and interviews conducted by Privacy International.

Privacy International is solely responsible for the content of this report.

OPEN SEASON

Building Syria's Surveillance State

December 2016

PRIVACY
INTERNATIONAL

www.privacyinternational.org

Table of Contents

Acronyms	5
Executive Summary	6
Building Syria's Surveillance State	8
Friends and middlemen	11
To capture, collect, analyse and store — in 'Country 4'	14
Filtering 'propaganda mail'	16
Monitoring the international exchanges in 'Lion country'	18
Satellite internet monitoring	21
Israel and geopolitics in the surveillance industry	23
War, Sanctions and Export Restrictions	26
The Hustle	30
Libya: a cash cow	32
Aftermath	34
Conclusion	36
Annex 1	38
Annex 2	43
Annex 3	46
Annex 4	48
Annex 5	49
Annex 6	68
Annex 7	70
Annex 8	73
Annex 9	75
Annex 10	77
Annex 11	79
Annex 12	80

List of Acronyms

DDOS	Distributed Denial of Service
ISP	Internet Service Provider
LIMS	Lawful Interception Management System (Utimaco)
PDN	Public Data Network
SCT	Syrian Communication Technology
STE	Syrian Telecommunications Establishment

Executive Summary

The Arab Spring of 2011 changed the political landscape of the Middle East and Gulf region. The scale of the popular uprisings seemingly caught off guard the governments of Syria, Egypt, and Libya among others, leading to brutal crackdowns and civil wars and instability that continue to this day.

Yet in the years leading up to this crisis, these governments spent millions of dollars developing sophisticated surveillance systems that they deployed against their citizens. PI obtained hundreds of original documents and pieces of correspondence related to the surveillance trade in this region leading up to and during the Arab Spring. Among these documents in particular is evidence of the Syrian government's ambitious plans and projects to monitor the national communications infrastructure, the technical details of which are revealed for the first time.

From 2007-2012, Syrian government built nationwide communications monitoring systems through at least four ambitious projects. Western businesses including RCS SpA (Italy) and VASTech (South Africa) were important contributors to Syria's repressive surveillance state while others including Amesys (France) competed for the opportunities on offer.

This report focuses as well on the vital role of middleman companies in the surveillance trade. These companies act primarily as resellers, brokers, logistics coordinators, and intermediaries between the surveillance technology manufacturers and their clients. They court and secure clients on the ground, smooth over logistical difficulties, and provide other services for a percentage of the total project. This report closely examines one such company, Dubai-based Advanced German Technology (AGT)¹, in enabling the construction of surveillance systems in Syria and further afield in the decade leading up to the Arab Spring revolts of 2011 and 2012.

In one transaction from 2008 and 2009, AGT in partnership with RCS proposed the use of US-origin equipment in a project to intercept communications on the networks of a satellite internet service provider, Aramsat, according to documents analysed by Privacy International. US sanctions and export control regulations in force at the time of this project restricted the exportation or re-exportation of certain US-origin goods to the country, including communications interception equipment. AGT claim that the project was never completed and that it follows all UN and EU export regulations. AGT's full response is included as an annex. RCS provided no comment related to the statements in the report.

¹ 'AGT' in this report refers to the Dubai-incorporated Advanced German Technology FZ-LLC through which the company conducts almost all of its business, rather than Berlin-based AGT GmbH.

chnology FZ-LLC through which ed Advanced German Technology

The Syrian government of president Bashar Al-Assad was intensifying its repression against dissidents and opposition groups at the same time as it was consolidating its surveillance capacities. Surveillance by both human and technological means was an important contributor to the repression that culminated in the 2011 crisis and ensuing civil war. To date, Al-Assad's government reportedly continues to maintain control over access to the internet and broadband and some of the surveillance architecture from these projects remains in place. The roles of several Western companies including AREA SpA (Italy) and Qosmos (France) who have been identified as selling surveillance technology to Syria have been the subject of inquiries in the US and France, respectively.

Other regional governments further afield engaged in repression of domestic political dissent also purchased similar technologies. AGT facilitated a particularly lucrative contract for the Libyan government of Colonel Muammar Gaddafi on behalf of South African surveillance company VASTech through consultants and companies. Funds from this project, among the most profitable for the company,² financed much of AGT's affairs. The lead up to the Arab Spring was an open season for surveillance companies – they provided technologies to eager government clients widely known to be publicly engaged in repression. They should share some responsibility for how their technologies are used.

Privacy International calls on export authorities to condition all exports of the surveillance technologies discussed in this report on rigorous, independent human rights impact assessments so as to minimize the potential that these technologies will be abused.

² Between 2005 and 2012.

Building Syria's surveillance state

The Syrian government commissioned its first nationwide monitoring system in 1999. The system, commissioned by the Syrian Telecommunications Establishment (STE), was designed to monitor mobile and fixed-line telephony and internet.³

TELECOMMUNICATIONS IN SYRIA

Two companies provide the country's mobile services – Syriatel and the Syrian subsidiary of South African-owned MTN. Syriatel is locally owned – one of its main investors and its CEO is businessman Rami Makhoul, a cousin of President Bashar al Assad⁴. MTN is a subsidiary of MTN of South Africa.⁵ Internet penetration is relatively low, reportedly at 28%.⁶ Many Syrians use internet cafes, where service is provided by around a dozen local internet service providers (ISPs).⁷

The Government maintains tight control of telecoms services through the telecom regulator and owner of the nation's telecommunications infrastructure, Syrian Telecommunications Establishment (STE).⁸ The use of censorship technologies to filter political, social, and religious websites, and to conduct surveillance on citizens is widespread. Targeted cyberattacks including general phishing, more targeted 'spear-phishing', the use of malware and 'Trojan horse' viruses against individuals and organizations; and distributed denial of service (DDoS) attacks against websites are widespread.⁹ Journalists and activists have been identified using these tactics and subsequently arrested.¹⁰ Web censorship is rife – STE blocked access to websites related to groups opposed to the al-Assad governments, human rights groups, the Muslim Brotherhood, and the country's Kurdish minority. Various Syrian telecommunications actors, including the Minister of Telecommunications and Technology and Syriatel CEO and Syriatel itself were respectively added to US sanctions lists in 2008 and 2011.¹¹

- ³ "Technical Specifications for the National Internet Backbone and STE ISP", Syrian Telecommunications Establishment, 1999, available at http://surveillance.rsfor.org/wp-content/uploads/2013/03/bidinvitation_ex.pdf
- ⁴ "President Assad And The Syrian Business Elite", Forbes, 30 March 2011, <http://www.forbes.com/sites/zinamoukheiber/2011/03/30/president-assad-and-the-syrian-business-elite/#d4431a55738c>
- ⁵ "Ericsson Region Middle East, Country Report: Syria", Ericsson, 2010, http://www.marconi.ca/tr/partners/documents/country_reports/SYRIA.pdf
- ⁶ "Freedom on the Net: Syria", Freedom House, 2015, <https://freedomhouse.org/report/freedom-net/2015/syria>
- ⁷ "Freedom on the Net: Syria", Freedom House, 2012, <https://freedomhouse.org/report/freedom-net/2012/syria>
- ⁸ "Freedom on the Net: Syria", Freedom House, 2012, <https://freedomhouse.org/report/freedom-net/2012/syria>. See also "Ericsson Region Middle East, Country Report: Syria", Ericsson, 2010, http://www.marconi.ca/tr/partners/documents/country_reports/SYRIA.pdf
- ⁹ "Freedom on the Net: Syria", Freedom House, 2015, <https://freedomhouse.org/report/freedom-net/2015/syria>. See also "New malware based attacks hit opponents in Syria and all over the world", Security Affairs, 20 August 2014, <http://securityaffairs.co/wordpress/27648/cyber-cri-me/rats-against-opponents-syria.html>
- ¹⁰ "Don't get your sources in Syria killed", Eva Galperin for Committee to Protect Journalists, May 2012, <https://cpj.org/blog/2012/05/dont-get-your-sources-in-syria-killed.php>
- ¹¹ "Treasury Sanctions State-Owned Syrian Financial Institutions and Syria's Largest Mobile Phone Operator", US Treasury, 10 August 2011, available at <https://www.treasury.gov/press-center/press-releases/Pages/tg1273.aspx> and "Rami Makhoul Designated for Benefiting from Syrian Corruption", US Treasury, 21 February 2008, available at <https://www.treasury.gov/press-center/press-release/s/Pages/hp834.aspx>

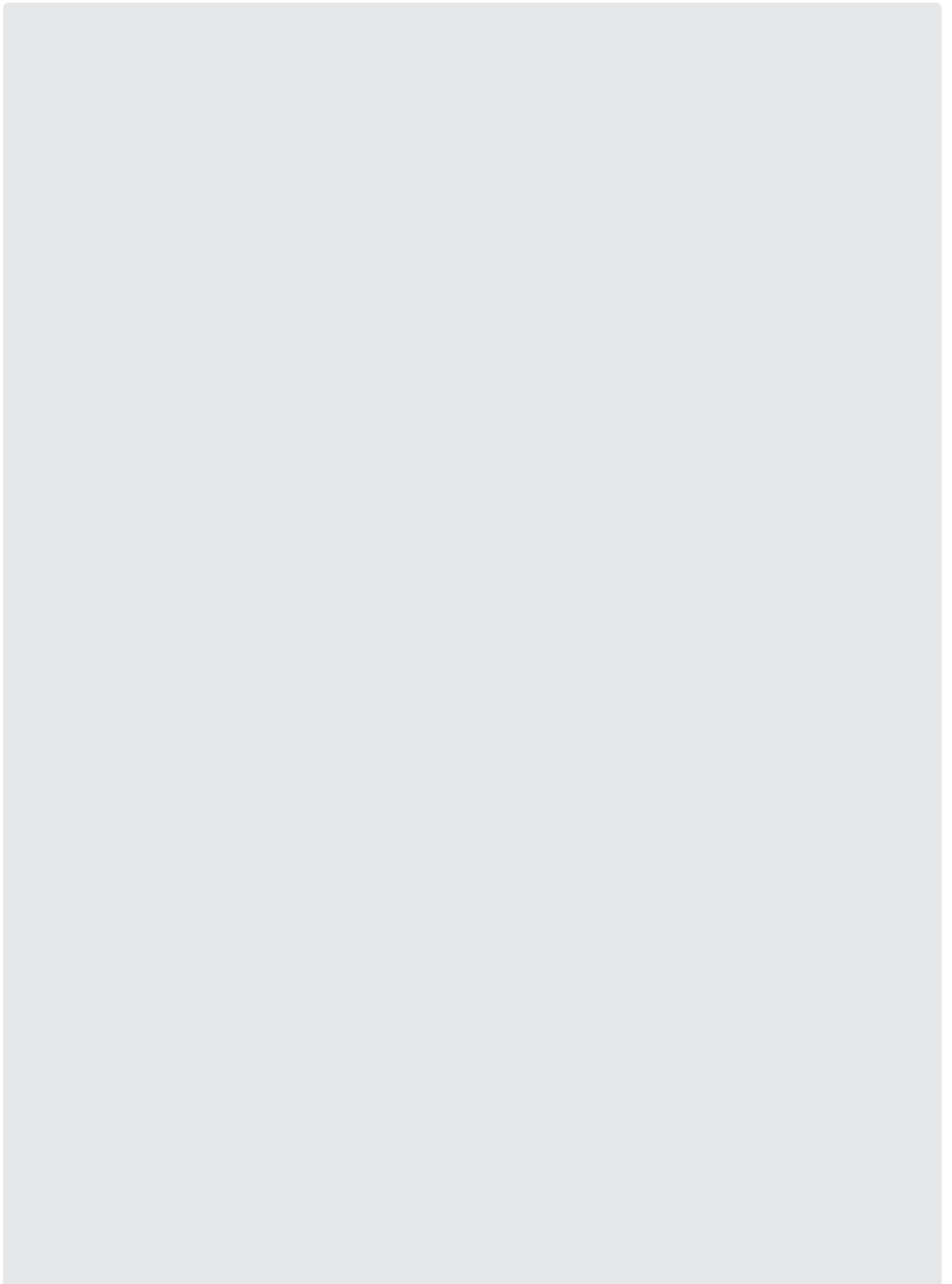
STE acted as a front for intelligence agencies, particularly the signals intelligence unit 'Branch 225', according to engineers familiar with lawful interception in Syria. "When I arrived at the international airport in Damascus, there were some guys from Syria secret services" recalls a network engineer who formerly worked in Syria. "They talked with me and they said that they were the real committer for this project." Another Syrian computer specialist recalls that communication service providers would have security officers attached to them that would approve intelligence agencies' requests for data: "They would come and collect the entire log...you would have to keep logs of your traffic for six months anyway, and you have to deliver that ... to the officer."

Communications surveillance, in conjunction with lower-tech surveillance strategies like the use of human informants and more traditional video and photo surveillance, was a key strategy of government control, both before and during the civil war, which began in 2011. This report focuses on communications surveillance — less observable than either physical surveillance or human intelligence gathering — and how the al-Assad government invested significant state funds and resources to automatically and passively collect, filter and analyse communications in Syrian territory directly from the national telecommunications architecture.

Since at least 2004, the Syrian government relied on technologies from German companies Siemens and Utimaco to intercept communications on these networks, according to documents obtained by Privacy International. In August that year, cybersecurity and surveillance technology firm Utimaco sold an interception management system to Siemens Syria for Eur 1.179 million, according to sales documentation from Utimaco. Its patented lawful interception management system, LIMS,¹² allows for the interception of communications in real-time. This includes phone calls, text messages, faxes, e-mails, VoIP calls, instant messaging and other services. The LIMS can be integrated into an existing telecommunications infrastructure and is compatible with a range of network providers. The LIMS provided to Siemens Syria was to be integrated into Syriatel networks and was present until at least 2009. Utimaco's LIMS were deployed to access those parts of Syria's network infrastructure that are provided by telecommunications infrastructure providers Nokia Siemens Networks (NSN) and Huawei. On parts of the network relying on infrastructure from Swedish provider Ericsson, Ericsson's own interception management interface was used, according to tender documentation. Utimaco states that there are no current installations of Utimaco's LIMS system in networks in Syria and no systems under license, support or maintenance by Utimaco or any of its partners. Utimaco's response is included as an annex.

By 2007, Assad's government was poised to massively expand its surveillance capacity. The original system had stopped working — updates to the Public Data Networks carrying Syria's telecommunications traffic meant that surveillance architecture needed to be kept up to date as well. The government was able to rely on a thriving industry of surveillance companies to service its ambitions.

¹² "LIMS Access Points", Utimaco, 2011, available at http://siii.transparencytoolkit.org/docs/Utimaco_LIMS_Product-Description-Specifications-1siii_documents



A diagram of the internet in Syria in 2009, from ST E tender documentation.
Obtained by Privacy International

Friends and middlemen

The surveillance industry comprises a complex web of companies in the supply chain from sale, installation and operation of communications surveillance projects.

On one end of the surveillance supply chain are the manufacturers of the heavy-duty and expensive components of surveillance systems like probes, interception gateways and monitoring centre components, including the monitoring consoles and data analytics software analysts use to query the raw telecommunications data. The majority of these companies are based in Europe, Israel, China, and the US, though a number of firms from countries including South Africa and India are gaining ground in the industry.

These firms rely on consultants and companies in the countries and region where they wish to do business to act as intermediaries. These 'brokers' court government agencies, engage in bids, resell equipment, facilitate customs and bureaucratic formalities, and otherwise secure the lucrative contracts for their partners, making a commission. They do this by entering into exclusivity agreements, and can incorporate new companies to act as vehicles for the surveillance contracts or extended business over time in a 'target' country.

Advanced German Technology (AGT) was one such intermediary. Founded by two Syrian-German brothers, Anas and Aghiath Chbib, the company reports that it had been providing surveillance and other technologies in Syria since 2002; it was ideally placed to benefit from the Syrian government's ambitious plans to expand its surveillance. In 2008 AGT registered a Syrian subsidiary, AGT Syria, with the Chbib brothers' uncle at the helm.

Gulf country clients at AGT's stall at a trade fair, 2005.
Obtained by Privacy International.

AGT

Despite its name, Advanced German Technology is actually based in Dubai and maintains a letterbox company in Berlin. It primarily resells digital forensic equipment and surveillance technology services. It was founded by two Syrian brothers, Anas and Aghiath Chbib, both of whom acquired German nationality. The elder, Anas (AGT's Managing Director) first star in the forensic and surveillance business as CEO of Instigo, a firm that went bankrupt in 2002.¹³ By 2003, Chbib was working with and then assumed directorship of a company called Isdon. Chbib had the company name changed to what it is now – Advanced German Technology FZ LLC — bought out his partners' shares, and transferred them to his shell company, Expert Consultant Ltd, registered in the British Virgin Islands tax haven Tortola. Expert Consultant is owned by both Chbib brothers. It is also owned by an offshore company linked to Jordanian-Swiss businessman Yahia Samawi Brascus Ltd.¹⁴ Samawi and members of his family¹⁵ are beneficiaries of Swiss-based professional services business, Brascus SA,¹⁶ which is also part owned by the offshore Brascus Ltd.¹⁷ In 2008, Brascus helped AGT court business from the Iraqi Minister of National Security.

AGT also acted as an intermediary for other larger surveillance companies. In 2008, AGT helped Stephane Salies, then-CEO of French surveillance technology firm Amesys via Allegretto Asset Management to set up an offshore company in the Ras Al Khaimah, an Emirate with a favourable tax regime. The other two shareholders of the new company were Abdlhakim Mudeer, a Libyan lawyer who assisted in the process of developing a nationwide interception project under then-president Muammar Gaddafi, and Anas Chbib. AGT characterize the company as being "related to some investment in the UAE in a very far sector from technology." [sic] Mudeer states that it was related to cybercrime. Salies stated that Allegretto is his personal investment company and that the company set up in Ras Al Khaimah had never been active as far as he is aware. Mudeer also denies involvement in the sale of surveillance technology. All responses received by PI related to the statements in the report by publication are included as annexes.

Two Chbib family members were on the payroll in Syria as consultants and several more paid for services rendered. AGT's internal accountants reported 'bonus'-marked payments to senior staff of over 4 million UAE dirham and unaccounted-for transactions, correspondence seen by Pri International.

-
- ¹³ "Instigo fails to appear in the Middle East", Arabian Business, 19 March 2012, <http://www.arabianbusiness.com/instigo-fails-appear-in-middle-east-206868.html>
- ¹⁴ "BRASCUS LTD.", Offshore Leaks Database, the International Consortium of Investigative Journalists, <https://offshoreleaks.icij.org/nodes/12133282>. Accessed September 2016.
- ¹⁵ "Yahia Samawi", Moneyhouse financial database, http://www.moneyhouse.ch/en/p/samawi_yahia-12867079/connections_zb.htm. Accessed September 2016.
- ¹⁶ "Brascus Aviation S.A.", Offshore Leaks Database, the International Consortium of Investigative Journalists, <https://offshoreleaks.icij.org/nodes/10128278>
- ¹⁷ In 2015. "EXPERT CONSULTANT LTD", Offshore Leaks Database, the International Consortium of Investigative Journalists, <https://offshoreleaks.icij.org/nodes/10154512>. Accessed September 2016. See also "Brascus SA Homepage", Brascus SA, <https://web.archive.org/web/20110128184525/http://www.brascus.com/>. Accessed September 2016.

To capture, collect, analyse and store — in ‘Country 4’

On 2 October 2007, the head of Syrian Telecommunication Establishment, Nazem Bahsas sent out a call to companies to tender for a new “Central Monitoring System for public data networks and the internet”. The tender specified that “the system must be centralized and has [sic] the ability to monitor all the networks which use data communication services inside the Syrian territories”.

The Central Monitoring System, according to tender documentation, would have to be able to capture and decode a wide range of personal communications services. An excerpt from the call for tenders is included as Annex 1.

‘Hot targets’ — specially designated communicating parties — could be monitored in real time. The bidding companies had to demonstrate that they would allow for 50 of these targets. The lag between collection of data and their availability for analysis on all targets would have been a few minutes at most.

The Central Monitoring System would be able to capture a wide range of personal communications services. Obtained by Privacy International.

One factor that distinguished the new system from the old was the alarming level of direct access that STE had to the nation's communications, independent of service providers' knowing cooperation. STE asked that "[a]ll monitoring activities should be done undetected, neither by the monitored targets, nor by ISPs, and not even by the management of the PDN [public data networks]". STE was seeking a system that was "immune against hacking, tampering or inspection of its content".

RCS S.p.A. — an Italian surveillance technology provider — jointly bid with AGT to provide the system.

RCS S.p.A

Milan-based RCS provides surveillance solutions to government clients worldwide. Formerly part of Urmet Group,¹⁸ it claims to have contributed to the interception of more than 10,000 targets daily in Europe alone.¹⁹ Its Italian clients include Telecom Italia and Vodafone Italy, according to project documentation. It offered three main products in the late 2000s — (1) the MITO monitoring centre, (2) the Internet Visualization System, a multimedia application for recording, storage, decoding, and presenting intercepted IP traffic, and (3) the Sfera investigation support system, to conduct automated analysis of very large subject-related databases.

RCS reportedly tendered in 2006 to provide an interception system to the government of Malta, but lost to Israeli rival Verint Systems, according to news reports.²⁰ In 2010 it offered to build a nationwide communications interception system for the Moroccan intelligence services, DGST. It is unclear if RCS won the contract.

After entering into an exclusivity agreement in September 2007, AGT spent the next few years pursuing this opportunity in Syria — codenamed 'Country 4'. Four RCS engineers would travel to Syria facilitated by AGT. By December, they were preparing to send their products in Syria to carry out the requested proof of concept, which included the real-time monitoring of Syrian targets. In April 2008, STE invited RCS and AGT to begin their pilot project, for the eagerly waiting STE. RCS engineers travelled to Damascus, Syria, staying in Le Meridien. One of them hoped, this time, to at last be able to use the pool. The demonstration was successful: STE asked the companies to submit their bid for the project.

STE was initially disappointed with the low levels of data being input into the proposed system, and AGT and RCS fought hard to keep their client's interest. They offered to sell an intrusion tool (G-Spy), AGT's answer to the more successful and well-known FinFisher intrusion malware, and throw in a few other sweeteners in a last-ditch bid to keep STE's interest. AGT deny possessing such technology. RCS's rival, Italian surveillance company AREA, would eventually win the project, according to correspondence seen by Privacy International and persons close to the project.

¹⁸ Urmet sold RCS SpA to the Sortrust in July 2008 following financial difficulties. "Sui titolari della società è giallo la proprietà è di una duciaria", La Repubblica, 3 December 2009, <http://ricerca.repubblica.it/repubblica/archivio/repubblica/2009/12/03/sui-titolari-della-societa-giallo-la-propriet>.html

¹⁹ "About Us," RCS SpA, accessed September 2016: <http://www.rcslab.it/en/about-us/index.html>

²⁰ "Unsuccessful Tenderer claims upgrade during tendering period led to contract award", Malta Independent, 6 August 2006, <http://www.independent.com.mt/articles/2006-08-06/news/unsuccessful-tenderer-claims-upgrade-during-tendering-period-led-to-contract-award-95039/>



A diagram of the internet in Syria in 2009, from ST E tender documentation.
Obtained by Privacy International

Filtering 'propaganda mail'

The Syrian government sought to centralize its persistent censorship of anti-government websites and install new capacities to censor and monitor politically inopportune speech. In December 2008, STE called for bids for the “supply, installation and operation of the equipment and software for content filtering required for Public Data Network Services (PDN) and the Internet.” Content filtering, in the context of communications traveling across the PDN and the internet, means analysing the communications data packets and assessing them for key words or attributes, and then either blocking transmission of that message, storing a copy for further analysis, or letting the message pass through without storage. Such technologies are also widely used for censorship, particularly at politically sensitive moments, such as during public protests. An excerpt from STE's requirements for the content filtering project is included as Annex 2.

Amesys, a French company who AGT called its partner in the bid, promoted its services to the Syrian government. Amesys controversially provided monitoring technology to the Libyan government in 2007. It is currently being investigated by the French courts for alleged complicity in human rights abuses including torture in Libya.²¹

AMESYS

Amesys is a French technology company, part of which telecommunications network surveillance technology. incorporated as a unit of Bull Group, which was in computing company Atos.²²

In 2011, Amesys was revealed to have provided a surveillance system to the Libyan government, according to documents seized by protestors from the abandoned security services following the 2011 uprising against then-President Muammar Gaddafi.²³ Following the scandal, Bull sold the interception wing of Amesys. A new, legally separate company Advanced Middle East Systems FZ LLC was established in 2012 in Dubai.

Amesys was a reliable partner of AGT – the two companies jointly organized ‘Defense Days’ workshops to train intelligence and law enforcement of officials from countries including Tanzania and South Africa, on forensic surveillance technologies. In 2008, AGT helped Stephane Salies, then-CEO of French surveillance technology firm Amesys via Allegretto Asset Management to set up an offshore company in the Ras Al Khaimah, an Emirate with a favourable tax regime. The other two shareholders of the new company were Abdh Hakim Mudeer, a Libyan lawyer who assisted in the process of developing a nationwide interception project under the deposed president Gaddafi, and Anas Chbib, a former member of the regime. Mudeer stated that Allegretto “related to some investment activity” and that the company set up in Ras Al Khaimah was “related to cybercrime.” Mudeer also denies involvement in the sale of surveillance technology. All responses received by PI related to the publication are included as annexes.

h specialized in
In 2010, Amesys was
turn bought by French

veillance system to the
protestors from the
sing against then-President
wing of
ddle East Systems FZ LLC was

anies jointly organized ‘Defense
rcement of cials from countries
d surveillance technologies. In
h surveillance technology firm
offshore company in the Ras
. The other two shareholders of
yer who assisted in the process
er deposed president Gaddafi,
ng “related to some investment
sity” Mudeer states that it was
o is his personal investment
ah had never been active as
in the sale of surveillance
the statements in the report by

²¹ “Amesys lawsuit (re Libya)”, Business and Human Rights Resource Centre, 2016, <http://business-humanrights.org/en/amesys-lawsuit-re-libya-0#c18496>

²² “Atos-Amesys S01E02 : à la recherche de l'éthique perdue”, Re ets.info, 18 March 2016, <https://re.ets.info/atos-amesys-s01e02-a-la-recherche-de-l-ethique-perdue/>

²³ “Firms Aided Libyan Spies,” The Wall Street Journal, 30 August 2011, <http://www.wsj.com/articles/SB10001424053111904199404576538721260166388>

016, <http://business->

8 March 2016, <https://re.ets.>

<http://www.wsj.com/articles/SB100>

"We are not concerned with "Classic" spam (such as junk mail for pharmacies online or whatever)," assured the STE Director General, "but rather with propaganda mail which has the shape of spam".

What kind of key 'propaganda' words did STE want a gged? "Given that we are not the authors of these messages, we cannot give a rm gure for the blocking criteria. Please specify the number that your proposed soluti on could handle currently along with the potential for expansion." It was not STE's call to make as to what constituted objectionable content — it was the end-user's, the Syrian intelligence services. By early 2010, the contract had still not been awarded. Salies, commenting on Amesys' business, con rmed that the company pursued business with AGT in Syria but denies that this particular opportunity was pursued further because of the political situation. Salies' full response is included as an annex.

Monitoring the international exchanges in 'Lion cou ntry'

In June 2009, the Syrian government announced an ev en more ambitious surveillance project — this time, to tap the two international e xchanges bringing internet traf c into the country in Damascus and Aleppo. The "Proje ct for supply and installation of Monitoring Equipment For the International Exchange s" would potentially allow for the

VASTECH

South African rm VASTech has been providing surveillance technology to government clients since 1999.²⁴ The company specialises in passive network interception products. By 2009 it had completed lawful interception projects in Syria, the broader Middle East, and North Africa. In 2011, VASTech was revealed to have provided its Zebra lawful interception syst em to the government of Colonel Muammar Gadda in Libya when operating manuals and other company-marked documents were recovered from the sta te security services building following Gadda's overthrow.²⁵ VASTech at the time declined to elaborate on the company's Libyan operations.²⁶

VASTech's founder Frans Dreyer died in a plane cras h outside Tripoli in May 2010, prompting some speculation as to whether the company would recover.²⁷ It strengthened its foothold in the Gulf in 2011 by es tablishing a company in Oman, VAS Tech LLC. VASTech has bene ted from public fund ing from the South African government²⁸ and by 2015, had expanded its business into other African countries, with of ces in Dubai and Switzerland.²⁹ The company's new product line includes Galaxia, a satellite monitoring system, Strata, for monitoring xed-line and mobile phone systems, and Portevia, for bre optic traf c monitoring.³⁰

²⁴ "Company Overview", VASTech, 2011. Available at https://wikileaks.org/spy/les/les/0/182_VASTECH-201110-BROCHURES.pdf

²⁵ "SA rm 'helped' Gadda spy on the people of Libya", Mail and Guardian, 2 Septe mber 2011, <http://mg.co.za/article/2011-09-02-sa-rm-helped-gadda-spy>

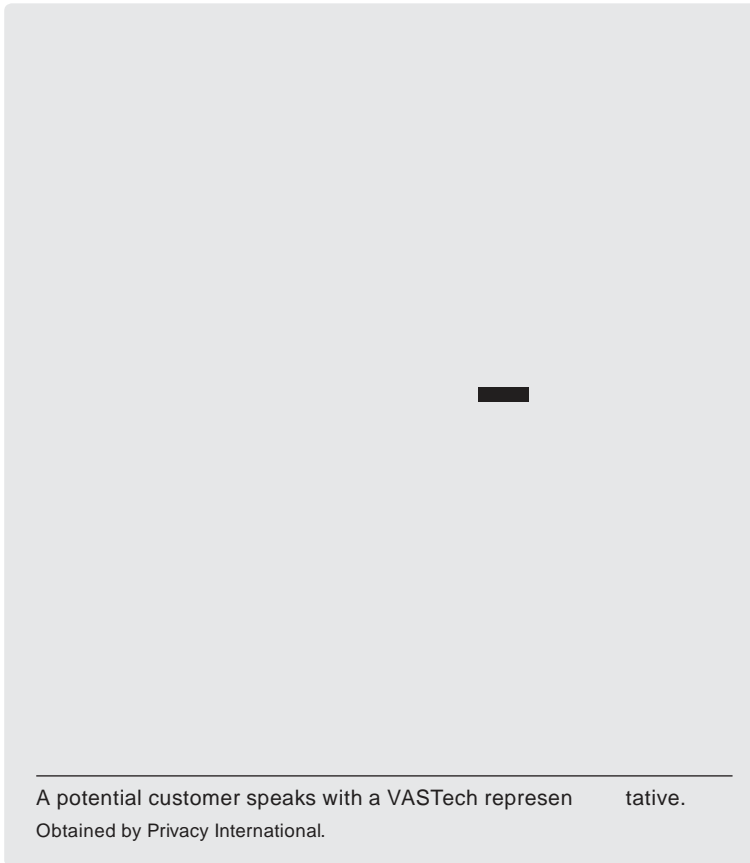
²⁶ "SA rm 'helped' Gadda spy on the people of Libya", Mail and Guardian, 2 Septe mber 2011, <http://mg.co.za/article/2011-09-02-sa-rm-helped-gadda-spy>

²⁷ "Say nothing – the spooks are listening", Mail and Guardian, 17 December 20 15, <http://mg.co.za/article/2015-12-17-say-nothing-the-spooks-are-listening>

²⁸ "South African Government still funding VASTech, knows previous nan cing was for mass surveillance", Privacy International, 30 January 2014, <https://www.privacyinternational.org/node/305>

²⁹ "ISS World 2016 MEA – Lead Sponsor", ISS World, http://www.issworldtraining.com/iss_mea/sponsors2h tml

³⁰ "Systems", VASTech, <http://www.VASTech.co.za/systems.html>. Accessed September 2016.



monitoring of all internet traffic into and out of the country.

This time, South African surveillance technology firm VASTech answered STE's call. They had a similar project running in the country since 2002.

VASTech has a close history with AGT. In July 2007, VASTech CEO Frans Dreyer took on the role of 'Technical Director' for AGT, according to a contract signed with AGT. VASTech deny that Dreyer ever held any position at AGT. VASTech had been providing interception capacity in Syria since 2002 — as part of its statement of intention to bid, the company confirmed that "the [AGT-

VASTech] consortium has 3 similar projects running, 1 in North Africa, 1 in the Middle East, and 1 in Syria (since 2002)." The North Africa project would later be revealed to be Libya.³¹

The Syrian government wanted to use 'brute force' speaker identification — tracking individual targets using Syria's phone services by comparing their unique voice prints against all calls into and out of and within Syria, which would be recorded. VASTech and AGT counselled them against this — the cost would simply be too high. Instead it recommended that the Syrian government apply 'focused' speaker identification which, "in combination with the VASTech Zebra Network Analysis capability, [would allow them] to search in a subset of the calls..." more likely to contain the target. An excerpt of the AGT-VASTech proposal for brute force voice identification of phone users in Syria is included as Annex 4.

VASTech tried hard to get the sensitive contract in Syria. Sales and marketing director Andre Scholtz and his wife travelled to Syria in mid-July 2010, facilitated by AGT's receptionist, who booked the VASTech delegation into the luxury Four Seasons resort for their stay in "Lion country", the code term for Syria. It is unclear whether VASTech won this particular contract. VASTech declined to comment on its business dealings in Syria and with AGT. On Libya, VASTech stated that it contracted lawfully in that country until terminating the agreement in February 2011. VASTech's full response is included as an annex.

³¹ "Firms Aided Libyan Spies," The Wall Street Journal, 30 August 2011, <http://www.wsj.com/articles/SB10001424053111904199404576538721260166388>

<http://www.wsj.com/articles/SB10001424053111904199404576538721260166388>

Of the protocols the system could decode would be multimedia files, HTTP (websites), various email services and web chat programmes. (25 August 2009)
Obtained by Privacy International

Satellite internet monitoring

By the late 2000s, the Syrian government had set up extensive infrastructure to intercept cable-bound communications traffic over much of the country. Yet in many more remote and rural areas ISPs relied on satellite providers, like Syrian provider Aramsat, to deliver connectivity to customers.

“This effortless usability accelerates the analysis, enabling the operator to find quickly on screen the most important pieces of the IP communication.”

RCS/AGT proposal to Syria Communication Technologies for satellite communications monitoring for Syrian law enforcement and intelligence (25 August 2009), Annex 5

The government also created a system to monitor these communications. RCS provided this capacity in 2009 after a successful demonstration of the product in 2008, according to company documentation including purchase orders and bank transfers. The complicated web of transactions involves companies in Italy, Kuwait, Syria, UAE and Cyprus, several of which are partially owned by Chbib using AGT's name, his business partner Mustafa Murad, an executive at Kuwaiti service provider Gulfsat, and Mohammed Mustafa Mero, a former Syrian politician.³² Murad and Gulfsat did not respond to repeated requests for comment.

The system was fitted with a probe that would be “passive,” receiving a copy of the “to be monitored” packet streams. It would then route these streams onward to Syrian law enforcement or intelligence agents via the monitoring system which would be physically located within “the central Law Enforcement Monitoring Facilities from which the LEA intends to decode and inspect the intercepted data.” Once the data was collected, a Syrian intelligence analyst could either archive the material for offline analysis at a later point, or follow a target live, as long as he/she was connected to the internet. The system was built to allow for the monitoring of “50 targets with 100 rules, using 10 client stations.”

“For the interception rate, the maximum value ever seen in all European and Extra-European countries is 1:2000...Considering the special context of this project, with the need of content-oriented monitoring, we considered for this project a very safe ratio of 1:1000.”

RCS/AGT proposal to Syria Communication Technologies for satellite communications monitoring for Syrian law enforcement and intelligence

documentation for satellite communications monitoring (25 August 2009), Annex 5

³² Mero held a 5 % stake of Syrian Communication Technology in February 2009, according to company registration information. Anas Chbib held 70 % of shares, with the remainder held by individuals who Privacy International was not able to identify.

documentation for satellite communications monitoring (25 August 2009), Annex 5

“[T]he system can [be] managed to monitor a bandwidth of 400MB [sic] without any extra charges to Gulf sat and it [sic] the requirements from the End User.”

Letter from AGT to Gulfsat, about the particular requirements of their Syrian end-user, (10 August 2008)

A PROFITABLE DEAL

Actor	Company	Country
Original equipment manufacturer	RCS proprietary equipment (software)	Italy (Milan)
	Dell and Netoptics are suggested for hardware	
Supplier	RCS SpA	Italy (Milan)
Partner	Advanced German Technology FZ-LLC	UAE (Dubai)
Contractor	Syrian Communication Technology (SCT) (jointly owned by Anas Chbib, Gulfsat, and various Syrian businessmen and politicians)	Syria (Damascus)
Client	Gulfsat (represented by Mustafa Murad)	Kuwait (Safat)
	NK Oriaka Communications Ltd (represented by Mustafa Murad)	Cyprus (Limassol)
End-User	Undisclosed Syrian law enforcement or intelligence agency	Syria

The actors involved in tapping communications over Aramsat's satellite networks.

Israel and geopolitics in the surveillance industry

Like many Middle Eastern governments, the Syrian government required its providers to demonstrate that they were completely free of ties to Israel. Foreign suppliers of surveillance technology and their domestic partners had to provide signed and notarised statements that their companies had no business dealings in Israel, no investment from Israelis or Israel-backed firms, and no intention to conduct business in Israel. The two countries have no formal diplomatic relations.

Companies were happy to oblige. “[W]e are pleased to do of cially con rm”, RCS reassured STE, “that RCS hasn’t sold / purchased to /from Israel any solution or part od [sic] solution relevant to Lawful Interception.” Similarly, VASTech declared its compliance with “the rules of Israel boycott.”

While diplomatic and trade relations between Israel and Gulf countries remain limited and discrete, several significant surveillance deals between Middle East and Gulf countries and Israel have been reported. AGT International, a Switzerland-based technology company with no apparent ties to Advanced German Technology but owned in part by prominent Israeli businessman Mati Kochavi, supplied a centralized, nationwide command and control system to the UAE government, according to Middle East Eye.³³

But geopolitical considerations would only matter so much. The successful bidder for one of the Syrian contracts, the Central Monitoring System, was AREA SpA. In December 2009, Anas Chbib drafted an error-lled letter — confidential and to be hand-delivered to STE head Nazem Bahsas — arguing that AGT and its own Italian partner RCS should have won the deal instead because they had the interests of the Syrian state at heart, unlike AREA which, Chbib claimed, had done business in Israel. The letter is included as Annex 3.

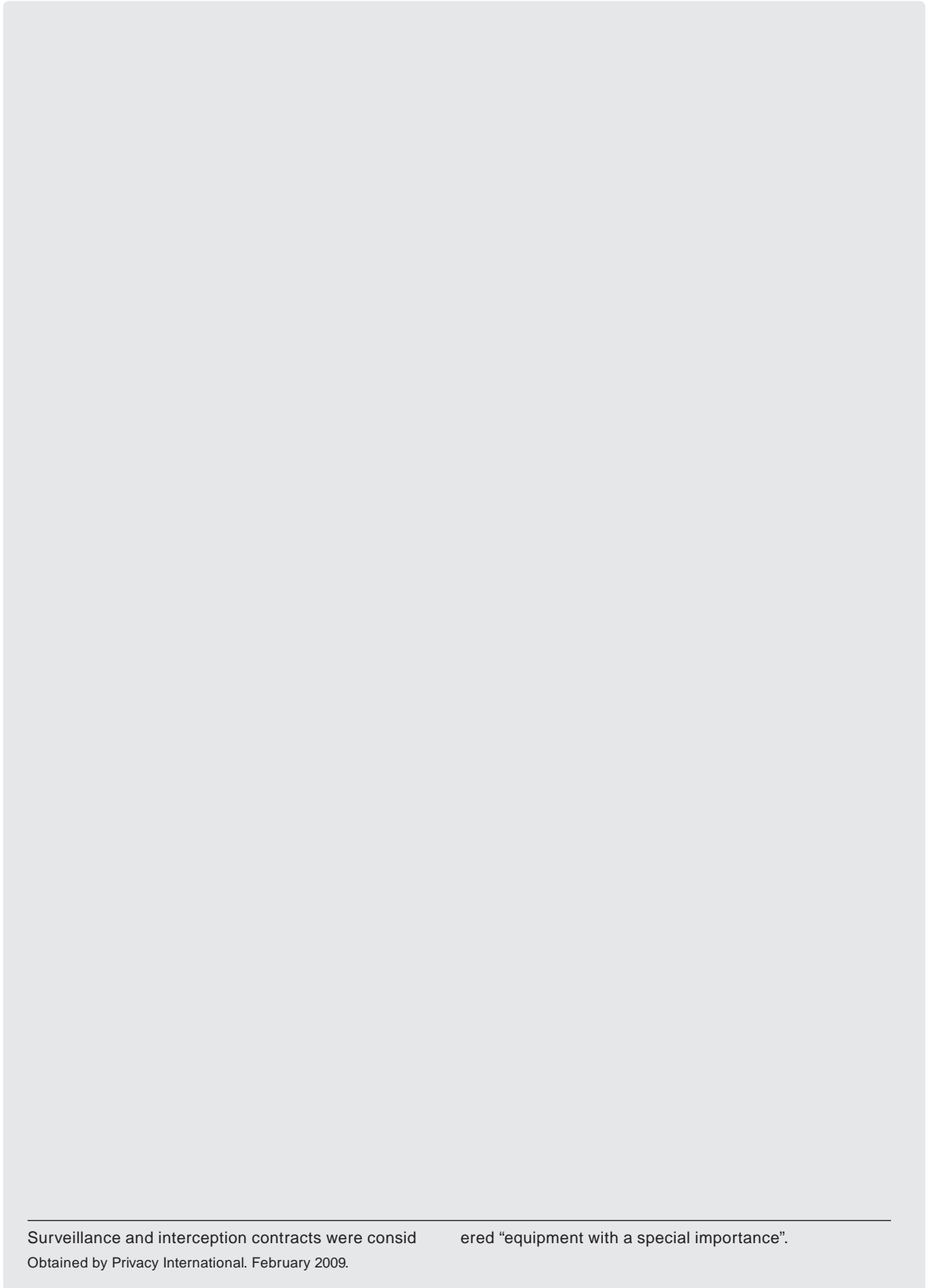
AGT was not successful in its appeal. Chbib probably never got his audience with President al-Assad. AREA continued its work setting up the central monitoring system project, codenamed Asfador, with partners German firm Utimaco and French company Qosmos.³⁴ But civil unrest caught the government and its surveillance technology providers by surprise. “[They were] in a hurry since they knew that sometime the revolution should be very near,” recalls the former network engineer.

³³ “Falcon Eye: The Israeli-installed mass civil surveillance system of Abu Dhabi”, Middle East Eye, 28 February 2015, <http://www.middleeasteye.net/news/uae-israel-surveillance-2104952769#sthash.sswIL7lp.dpuf>. The investigation was prompted by a mysterious routine fight between the two nations. “Secret fight linking Israel to the UAE reveals ‘open secret’ of collaboration”, Middle East Eye, 22 December 2014, <http://www.middleeasteye.net/news/secret-fight-between-israel-and-uae-567607953>

³⁴ “Syria Crackdown Gets Italy Firm’s Aid with U.S.-Europe Spy Gear”, Bloomberg News, 3 November 2011, <http://www.bloomberg.com/news/articles/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear>

Political sensitivities on display: AGT claims AREA undercut them and did not have Syrian national interests at heart.

Obtained by Privacy International. December 2009.



Surveillance and interception contracts were considered "equipment with a special importance".
Obtained by Privacy International. February 2009.

War, Sanctions and Export Restrictions

On 15 March 2011, protestors in Damascus took to the streets to demand democratic reforms and the release of political prisoners. By April 2011, the protests had turned to more explicitly anti-Assad protests. In the ensuing crackdown and skirmishes, by May the death toll had reportedly reached over 1,000.³⁵ The government lost control of much of the country's restive north and east, as rival militant groups claimed more and more territory in what is currently Syria's civil war.

The government's crackdown on the flow of information was almost immediate. In May 2011, the Ministry of Defence reportedly issued a communique ordering the disconnection of the internet in Homs and other restive areas of eastern Syria.³⁶ Researchers reported a full day, nationwide internet blackout in June 2011,³⁷ and more localized blackouts throughout Syria. Activists reported that when pro-regime forces would besiege a city, the broadband bandwidth was reduced dramatically and 3G services shut off.³⁸ Telecommunications infrastructure was also badly damaged in bombing campaigns, especially in cities like Homs that were subject to particularly severe shelling by the Syrian armed forces.³⁹

The EU and the US responded with new restrictions, including concerning the sale of interception equipment to the Syrian government. The US has considered the Syrian government a 'state sponsor of terrorism' for almost 30 years.⁴⁰ Extensive sanctions and export control regimes govern the kind of trade US businesses can legitimately conduct with the country. Executive Order 13338, signed by President Bush in 2004, placed a trade embargo on Syria prohibiting, without a license, the exportation or re-exportation of most US-origin goods to the country, including surveillance equipment.⁴¹

- ³⁵ "Syria death toll 'surpasses 1,000'", Al Jazeera, 24 May 2011, <http://www.aljazeera.com/news/middleeast/2011/05/2011524182251952727.html>
- ³⁶ "Leaked Syrian document shows how Assad banned internet access and satellite phones", Michael Weiss, Blog for The Telegraph, accessed September 2016: <http://blogstelegraph.co.uk/news/michaelweiss/1000-leaked-syrian-document-shows-how-assad-banned-internet-access-and-satellite-phones/> 93908/
- ³⁷ "Syria's Internet Blockage Brings Risk of Backfire", The Wall Street Journal, 3 June 2011, <http://www.wsj.com/articles/SB10001424052702304563104576363763722080144>
- ³⁸ "Freedom on the Net: Syria", Freedom House, 2012, <https://freedomhouse.org/report/freedom-net/2012/syria>
- ³⁹ "Freedom on the Net: Syria", Freedom House, 2012, <https://freedomhouse.org/report/freedom-net/2012/syria>
- ⁴⁰ "Syria Sanctions", US Department of State, accessed September 2016: <http://www.state.gov/e/eb/dfs/spi/syria/>
- ⁴¹ With the exception of certain medicines and food, Regulations ("EAR") may be exported or re-exported to Syria without a Department of Commerce license. The Department of Commerce's Bureau of Industry and Security ("BIS") administers the EAR, which controls exports and re-exports of a broad range of dual use goods and technology. 15 CFR §746.9, which contains the EAR provisions relating to Syria, provides that "all license applications for export or reexport to Syria are subject to a general policy of denial except that applications for technology and source code on the Commerce Control List (CCL) "will be reviewed on a case-by-case basis." (These controls were placed in 15 CFR §746.9 on December 12, 2011; Order No. 2, codified in Supplement No. 1 to Part 73 as a supplement to the EAR, lists certain types of telecommunications interception or jamming equipment surreptitious interception of wire, oral, or electronic communications, other than those controlled under 5A001.f.1" (5A980); and "cryptographic information security" equipment, including "information security" systems, equipment and "components" (5A002).

Since the uprisings began in Syria, the US government has issued a series of further restrictions on exports to Syria.⁴² In August 2011, President Obama announced new sanctions against Syria that further restricted the sale of interception equipment specifically — for the first time, Syriatel was added to the list of proscribed groups.⁴³ The European Union (EU) only enacted specific sanctions concerning the sale of telecommunications and surveillance equipment in 2011⁴⁴ and again in 2012.⁴⁵

Prior to and in tandem to these specific EU restrictions, the Wassenaar Arrangement would have governed exports of surveillance technology to Syria from countries who are participants to it. The Wassenaar Arrangement is a multi-governmental trade control regime in which participants agree what conventional weapons and dual-use goods should be controlled in order to promote international security. Crucially, the 41 participants include five out of the world's six biggest arms exporters - the US, Russia, Germany, France and the UK.⁴⁶

Companies were aware of restrictions on technology exports to Syria but nevertheless appeared open to supplying surveillance technologies to the country.

In 2010, it appears AGT was prepared to sell Silent runner probes of US technology firm AccessData to one of Syria's two mobile service providers, MTN Syria.⁴⁷ US sanctions and export control regulations in force at the time of this transaction restricted, without

⁴² Executive Orders 13572, 13573, 13582, 13606, 13608.

⁴³ "Treasury Sanctions State-Owned Syrian Financial Institutions and Syria's Largest Mobile Phone Operator", US Department of the Treasury, 10 August 2011, <https://www.treasury.gov/press-center/press-releases/Pages/tg1273.aspx>

nd Syria's Largest Mobile Phone
[https://www.treasury.gov/press-center/press-](https://www.treasury.gov/press-center/press-releases/Pages/tg1273.aspx)

⁴⁴ "The sale, supply, transfer or export of equipment or software intended for monitoring or interception by the Syrian regime, or on its behalf, of the Internet communications on mobile or fixed networks in Syria and the provision of assistance to install, operate or update such equipment or software shall be prohibited." Council Decision 2011/782/CFSP of 1 December 2011, art. (3), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJL_2011_319:0056:0070:EN:PDF

rimarily for use in the
Internet and of telephone
assistance to install,
Council Decision 2011/782/
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJL_2011_319:0056:0070:EN:PDF)

⁴⁵ "The competent authorities of the Member States, as identified in the website Annex III, shall not grant any authorisation under paragraph 1 if they have determined that the equipment, technology or software in question would be used for monitoring or interception, by the Syrian regime or on its behalf, of internet or telephone Syria." Council Regulation (EU) No 36/2012 of 18 January 2012, art. 4(2), available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJL_2012_016:0001:0032:EN:PDF

tes referred to in
reasonable grounds to
be used for monitoring or
communications in
available at [http://eur-lex.](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJL_2012_016:0001:0032:EN:PDF)

⁴⁶ The Wassenaar Arrangement has for decades controlled the export of cryptography, meaning that some if they contain certain levels of cryptography. In 2010, "laser microphones" were added to list, which are used to eavesdrop on conversations by listening through glass. In 2012, phone monitoring technology was explicitly added to the Wassenaar list to target mobile and satellite phone monitoring equipment. Prior to 2012, some states had already controlled the equipment because of controls related to 'Telecommunications systems, equipment, components' though this was interpreted differently by participating states. In 2013, further categories were added to the Wassenaar control list: intrusion software and IP surveillance systems. The EU is currently undergoing a revision of its Dual Use Regulation, which among other things, incorporates the Wassenaar control list into an EU control list used by member states. See, for example, "Final Report on the Review of the EU Dual-Use Export Control Policy", European Commission, http://ec.europa.eu/external_relations/legislation/legislation/FINAL_REPORT.pdf and "Summary of Changes: List of Dual-Use Goods & Technologies of the Wassenaar Arrangement", accessed September 2016, <http://www.wassenaar.org/wp-content/uploads/2015/06/Revised-Summary-of-Changes-to-Control-Lists.pdf>

d the export of cryptography, meaning that some
if they contain certain levels of cryptography.
which are used to eavesdrop on conversations by
listening through glass. In 2012, phone monitoring
technology was explicitly added to the Wassenaar list
to target mobile and satellite phone monitoring
equipment because of controls related to 'Telecommunications
systems, equipment, components', though this was interpreted
differently by participating states. In 2013, further categories
were added to the Wassenaar control list: intrusion
software and IP surveillance systems. The EU is currently
undergoing a revision of its Dual Use Regulation, which
among other things, incorporates the Wassenaar control list
into an EU control list used by member states. See, for
example, "Final Report on the Review of the EU Dual-Use
Export Control Policy", European Commission, http://ec.europa.eu/external_relations/legislation/legislation/FINAL_REPORT.pdf and "Summary
of Changes: List of Dual-Use Goods & Technologies of the
Wassenaar Arrangement", accessed September 2016,
<http://www.wassenaar.org/wp-content/uploads/2015/06/Revised-Summary-of-Changes-to-Control-Lists.pdf>

⁴⁷ MTN Syria had been in possession of US technology for some time. Syrian employee of Areeba, a Syrian provider which merged with the MTN group, assured AGT it would be able to have US software, even that they were in possession of Cisco servers. Cisco had previously told CBS News that it had a "few licensed sales" to MTN Syria, but said it was "sanctioned" by the U.S. government. See also "Surveillance and censorship: Inside Syria's Internet", CBS News, 12 December 2013, <http://www.cbsnews.com/news/surveillance-and-censorship-inside-syrias-internet/>

ees of Areeba, a
ve US software,
CBS News that it
government. See
ws, 12 December 2013, [http://www.](http://www.cbsnews.com/news/surveillance-and-censorship-inside-syrias-internet/)

Financial Proposal: Network-Data Monitoring and File & LAN Encryption

Offer date: 11. Jan 10

Offer no: 01-M-01

Offer to:		Ship to:	
Company name:	MTN South Africa	Company name:	MTN South Africa
Contact person:		Contact person:	
Address:		Address:	
Address 2:		Address 2:	
Postal code:		Postal code:	
City / Country:	Johannesburg / South Africa	City / Country:	Johannesburg / South Africa
Telephone number:		Telephone number:	
Fax number:		Fax number:	
E-mail:		E-mail:	
Vat no:		Notes:	

Specification			
Currency:	USD	Express Shipment	No
Terms of payment:		Standard Shipment	Yes
Sales code:	MR	Terms of delivery	DDP
		Discount approved by	

Products					
Art no	Description	Units	Price per unit		Total
Safeguard LAN Crypt	File Encryption Solution	100	119,80		14.094,12
Safeguard MailGateway Professional	Email Encryption Solution	100	50,40		5.929,41
Support for Sophos products	Support for Sophos Products (one unit for two)	100	17,02		2.002,35
SilentRunner	Real-Time Network Data Observation Solution (all components included except laptop)	1	58.823,53		58.823,53
Support for Silent Runner (1 year)	Support for Silent Runner (1 year)	1	11.764,71		11.764,71

A financial proposal from AGT states the destination as South Africa. The proposal was attached to an email discussing sending the equipment for use in Syria. Obtained by Privacy International.

a licence, the exportation or re-exportation of US- origin communications equipment to Syria, which would almost certainly include probes of the type manufactured by AccessData. In January 2010, AGT's Director of Sales and Marketing Marco Rettig offered to route the shipment of cially from Dubai through MTN's parent company in South Africa. In email correspondence with senior MTN Syria employees, he appears to propose this method in order to avoid export restrictions to Syria.

“We have thoroughly screened the market for an appropriate solution and have spoken to many (!) different suppliers. Unfortunately, all solutions that would have fulfilled your requirements technically where SUBJECT TO EXPORT RESTRICTIONS to Syria! The alternative would have been inferior products that would not suffice your expectations. Therefore, we believe the BEST WAY IS TO DELIVER THE PRODUCT TO MTN SOUTH AFRICA.”

Email from Marco Rettig, AGT Director of Sales and

Marketing to Husam Sidawi and

Wassim Saad, MTN Syria, 11 January 2010. Emphasis i

n original.

AccessData denies knowledge of the AGT proposal. AccessData's full response is included as an annex. Email correspondence within AGT suggests that US companies including AccessData did not wish to consider doing business in Syria and Libya. If this transaction were in fact completed, as AGT proposed in 2010, it may have violated US sanctions and export control regulations. AGT states that it has been following all UN and EU export regulations. AGT further stated in relation to the AccessData probes: "its the vendor responsibility to obtain the export license, and not the seller, and at the end its south African company, MTN is telecom operator with many location and licenses, if they wanted to use network forensic tool to identify any malware in the network, than its internal issue, this tool is not been made be installed on public networks." [sic] MTN state that though a proof of concept process was proposed to be undertaken in South Africa, MTN Syria did not procure any products from AGT. MTN's response is included as an annex.

In another project, beginning in 2008, AGT suggested the inclusion of US-origin equipment in a project to intercept communications on the networks of a satellite internet service provider, Aramsat, as described above. A July 2008 list of hardware considered for the demo phase of the project includes network probes by US-headquartered Netoptics. An August 2009 technical proposal from an AGT-RCS partnership to SCT for the full phase of the project specifies US-origin hardware for the project: it lists Dell Xeon Intel servers (DELL PE2950) as part of the "proposed TIP probe" and "backend IVS (internet visualization system)". The proposal is included as Annex 5.

RCS did not include hardware in their own June 2008 offer to AGT, according to project documentation reviewed by Privacy International.⁴⁸ These specifications raise the question of whether there was an intent to provide US-origin hardware for the project and how that hardware would be procured.

RCS did nevertheless suggest a minimum configuration based on specific US-origin technology for the interception project in Syria throughout the project's demo and full phase. Purchase orders for software for the project were fulfilled in October 2009. It is not clear what hardware was actually procured for the project. If a company were in fact actively involved in procuring, preparing and providing US-origin equipment for an interception project in Syria, it may have acted in violation of US sanctions and export control regulations. US sanctions and export control regulations in force at the time of this project restricted the exportation or re-exportation of such US-origin goods.⁴⁹

AGT states that network surveillance technology from RCS was not sold for the Aramsat monitoring project. AGT further states in relation to this project: "never sold, and if its offered the HW [hardware], it is local supply issue, and we can not, will not involve in any importing of HW like dell or others, to any country, not only Syria, beside it was available in SYRIA without any involvement of AGT, as we are not hardware vendor nor distributor." [sic]

⁴⁸ The 11 June 2008 offer letter for the project's demo phase states: "Hardware is not part of the present offer. RCS suggest [sic] minimum configuration detailed in the annexed documents".

⁴⁹ See note 41.

"I know from how I was working ... there was absolutely no due diligence on who they [AGT] were supplying to," recalls a former technical AGT employee. "And that's the way it was done, there was never any checks carried out."

Another engineer not affiliated with AGT who worked in Syria recalls that routing controlled technologies through Dubai diverted attention from where, exactly, these technologies were ending up: "When I was in Syria, I saw a ton of different USA brands, Cisco, IBM and all of them arrived from Dubai".⁵⁰

⁵⁰ Privacy International was unable to independently verify claims that Cisco and IBM equipment supplied in Syria.

The Hustle

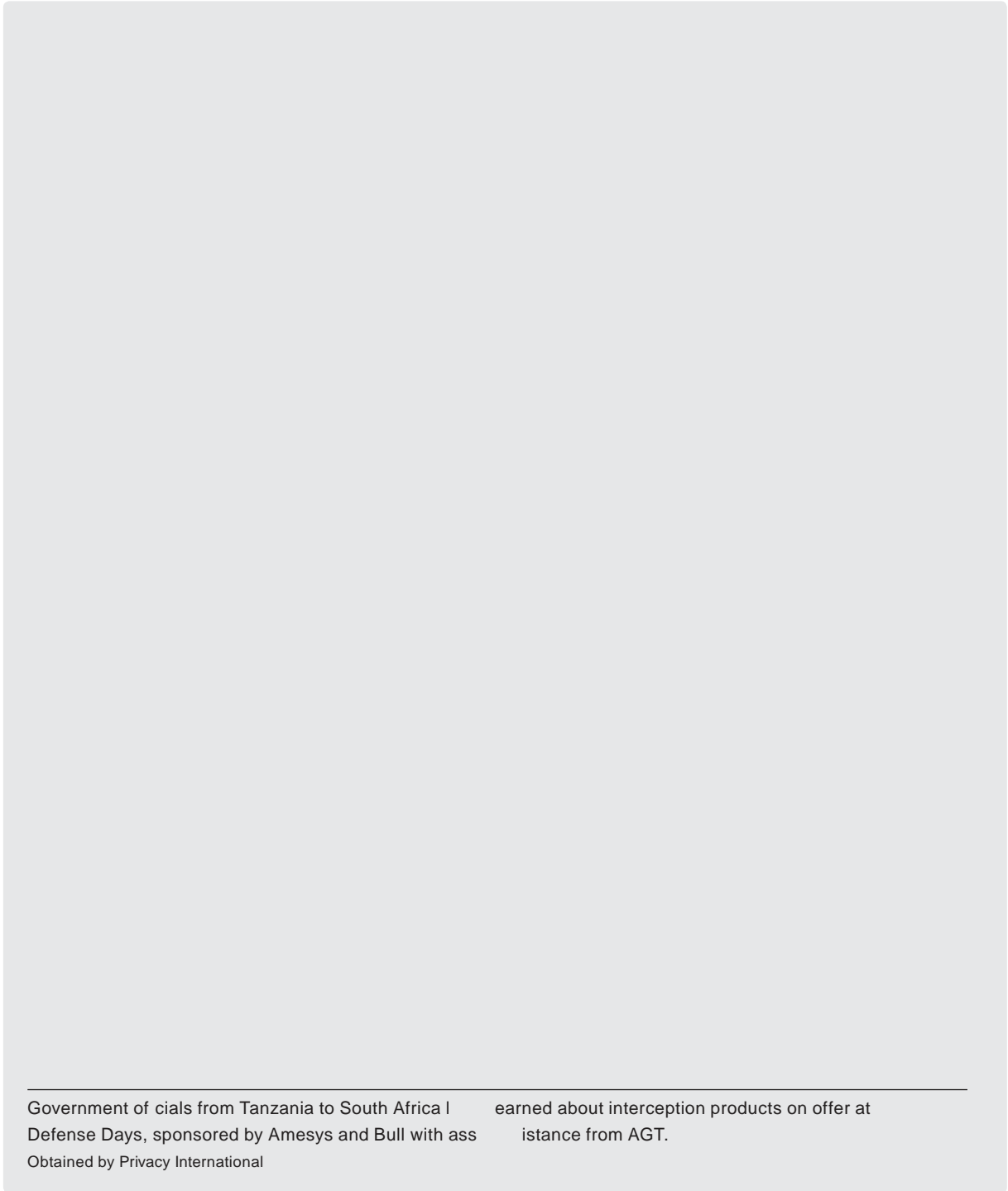
During the late 2000s, governments across the Middle East and North Africa faced increasing domestic unrest. By mid-2011, Bahrain, Egypt, Libya, Syria, Tunisia, and Yemen were facing full blown uprisings. In the run-up to this unrest, their governments had been willing to buy whatever might help them regain control — including more surveillance technologies.

Fortunately for AGT, the region was its area of expertise. Its clients for both surveillance and other technology projects in 2010 included governments of Saudi Arabia, Kuwait, UAE, Jordan, Egypt, Bahrain and Qatar. AGT also attempted to cultivate business in Sudan, arranging to meet in Dubai with Presidential advisor and former head⁵¹ of Sudan's National Security and Intelligence Service, Salah Abdallah Gosh in 2011. Gosh has been accused of having a significant role in organizing the Sudanese government's support to militias in the Darfur conflict.⁵² AGT deny meeting Gosh, stating they have never done business with either Sudan or South Sudan.

Doing business at an international military and police technology trade show in 2015.
Obtained by Privacy International.

⁵¹ "Sudanese president names new intelligence chief," Al Arabiya, 14 August 2009, <http://www.alarabiya.net/articles/2009/08/14/81753.html>

⁵² "The Foreign Office, Sudan's secret police chief, and the war on terror", The Independent, 26 November 2006, <http://www.independent.co.uk/news/world/politics/the-foreign-of-ice-sudans-secret-police-chief-and-the-war-on-terror-6229800.html>



Government officials from Tanzania to South Africa learned about interception products on offer at Defense Days, sponsored by Amesys and Bull with assistance from AGT.
Obtained by Privacy International

Libya: a cash cow

On 15 February 2011, up to 2,000 people took part in overnight protests against the arrest of a prominent government critic and lawyer. Dozens of protesters were killed in fighting between security forces and the protesters. Nine months later, in October, the National Transitional Council declared the country 'liberated', as Gaddafi's government had been earlier forced out of the capital Tripoli, and Gaddafi killed. The civilian death toll numbered in the thousands.

Documents seized in 2011 from Libya's security services confirmed that VASTech had provided communications surveillance capacities to the government.⁵³ Behind the scenes, in the two years leading to the revolution, AGT had facilitated a surveillance project⁵⁴ codenamed 'Mehari', according to documents obtained by Privacy International. But the project largely consisted of facilitating VASTech's interests in Libya.

Company accounts reveal that AGT received over 7.9 million UAE dirham (approximately 1.3 million UK Pounds) between late 2009 and late 2011 marked for a 'Mehari' project. Persons familiar with the payments stated that it was a "paper project" — that the majority of funds VASTech provided to AGT were paid out in consulting invoices to third parties for facilitating VASTech's business in Libya rather than a technical project AGT was responsible for implementing. AGT assisted when VASTech ran into difficulties importing equipment into Libya, according to company accounts and a person with knowledge of the project. Financial records show no indication that 'Mehari project' funds were used to procure any physical equipment or software.

AGT and VASTech did not respond to requests for clarification on the Mehari project. VASTech stated that the company withdrew from Libya in 2011.

The funds provided from this project did, however, allow AGT to finance other parts of the company and pay off urgent bills from increasingly angry creditors. The Libyan funds allowed AGT to continue paying various members of the Chbib family in Syria. A cousin of the family made 25,000 UAE per month (around 50,000 UK Pounds per year) for 'business development' work at AGT. This was still under half of the company director's own salary, excluding the ample housing, car, and holiday allowances the company already paid. Samer Chbib, the Chbib brothers' uncle, facilitated much of AGT's work in Syria and handled large transfers for an 'STE project' in January and February 2010 and throughout the year. At least two other Chbibs based in Syria were engaged prominently in translation and other consulting services.

⁵³ "Firms Aided Libyan Spies," The Wall Street Journal, 30 August 2011, <http://www.wsj.com/articles/SB1001424053111904199404576538721260166388>

⁵⁴ From December 2009 to January 2010, VASTech ME FZE paid over 5.8 million UAE dirhams (around 978,000 UK Pounds) to AGT. Together this comprised the 'commission' fee AGT received for facilitating the 'Mehari' project. Part of the total sum was paid onward in 'consulting fees' to individuals or companies whose identities Privacy International was unable to confirm. In July 2010, VASTech's Frans Dreyer travelled to Tripoli to 'have a meeting with Mahari [sic] as part of a regional tour. Mehari — whether referring to a person, a team of people, or an institution — was also referred to as 'Mahari' reigners, the 'Radisson Blu Mahari'. AGT received a further sum of approximately 360,000 UK Pounds from VASTech mostly in October 2011. AGT paid out almost all of this in two separate cheques dated one month before earmarked for a "Mehari project".

<http://www.wsj.com/articles/SB1001424053111904199404576538721260166388>

rhams (around 978,000 UK Pounds) to AGT. Together this comprised the 'commission' fee AGT received for facilitating the 'Mehari' project. Part of the total sum was paid onward in 'consulting fees' to individuals or companies whose identities Privacy International was unable to confirm. In July 2010, VASTech's Frans Dreyer travelled to Tripoli to 'have a meeting with Mahari [sic] as part of a regional tour. Mehari — whether referring to a person, a team of people, or an institution — was also referred to as 'Mahari' reigners, the 'Radisson Blu Mahari'. AGT received a further sum of approximately 360,000 UK Pounds from VASTech mostly in October 2011. AGT paid out almost all of this in two separate cheques dated one month before earmarked for a "Mehari project".

Libyan business was good but risky money. “[P]lease do not give any Country Name... No country name or clients,” Chbib advised one staff member in an email about Libya seen by Privacy International. Many employees were kept in the dark about the company’s work outside of their own narrow area, recalled several former employees. “[Anas] Chbib told us not to talk about anything that was going on outside of what we were working on,” recalled a former technical employee. “So when we knew he was going to Libya, this sort of thing, we weren’t allowed to discuss that.” Chbib continued to travel on the ‘Mehari’ project in late 2011, and into 2012. Libya’s fledgling transitional government was struggling to control the country. Fighting erupted two years later, returning Libya to civil war.

Aftermath

The conflict in Syria devastated much of its communications infrastructure. Among the massive population outflux were many of its skilled engineers. Security forces arrested activists and suspected government opponents en masse; hundreds would be arrested, tortured or disappeared. The Syrian Electronic Army, a pro-government hacker militia, engaged in widespread cyberattacks against activists and anti-government groups. Targeted malware, hacking⁵⁶ and 'man in the middle' attacks⁵⁷ have also been used to identify and spy on dissidents.

The surveillance infrastructure in Syria is still in place, but it is only partially effective and being managed albeit not very effectively by Syrian staff, according to two persons close to the project. The most difficult and complex part of the system to maintain — the probes — requires maintenance that is difficult to accomplish in a highly volatile region where sabotage and damage to the network is rife.⁵⁸

AREA, the Italian company who won one of the major surveillance infrastructure contracts, claims it halted work on the Syrian system.⁵⁹ It was also forced to pay a fine to the US Department of Commerce for violating US export control regulations.⁶⁰ The company is still active in the Middle East. In June 2016, the Italian government granted AREA a license to export surveillance technology to Egypt,⁶¹ despite an EU joint motion several months prior calling for a suspension in exports of surveillance equipment⁶² to Egypt in light of the murder of an Italian doctoral student allegedly at the hands of Egyptian security forces. Italian police raided AREA's offices in December 2016, suspecting violations of European embargoes.⁶³ Meanwhile, AREA's partner in the Syria project, French company Qosmos, is being investigated by the French courts for possible complicity in torture. The results of that case are still pending.⁶⁴

- ⁵⁶ "Behind the Syrian Conflict's Digital Front Lines", FireEye Special Report, 2015, <https://www.reeye.com/content/dam/reeye-www/global/en/currentthreat/s/pdfs/rpt-behind-the-syria-conflict.pdf>
- ⁵⁷ "A Syrian Man-In-The-Middle Attack against Facebook", Electronic Frontier Foundation, 5 May 2011, <https://www.eff.org/deeplinks/2011/05/syrian-man-middle-against-facebook>
- ⁵⁸ "People also managed to work around the government's network surveillance. One computer specialist recalls: "DPI, deep packet inspection, the government benefited from it. It was effective, but going around it took only 10 days after that, and it became known how to go around it.... People would also change, defect with the crisis, within the STE, they were pro-change, so a lot of these services were effected."
- ⁵⁹ "Italian Firm Said to Exit Syrian Monitoring Project", Bloomberg, 9 November 2011, <http://www.bloomberg.com/news/articles/2011-11-09/syrian-monitoring-project-may-end-as-italy-irm-weighs-options> (accessed May 2016)
- ⁶⁰ "Italian Company Agrees to \$100,000 Penalty for Unlawful Technology Export to Syria", US Department of Commerce, 17 September 2014, <https://www.bis.doc.gov/index.php/about-bis/newsroom/press-releases/107-about-bis/newsroom/press-releases/press-release-2014/643-italian-company-agrees-to-100-000-penalty-for-unlawful-technology-export-to-syria>
- ⁶¹ "L'Italia esporterà software di sorveglianza in Egitto", La Stampa, 28 June 2016, <http://www.lastampa.it/2016/06/28/italia/italia-esporter-software-di-sorveglianza-in-egitto-11iR9uYFcPpkP9PebyHdwM/pagina.html>
- ⁶² "Joint Motion for a Resolution", European Parliament, 9 March 2016, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP/TEXT+MOTION+P8-RC-2016-0338+0+DOC+XML+V0/EN>
- ⁶³ "Italian Cops Raid Surveillance Tech Company Accused of Selling Spy Gear to Syria", VICE Motherboard, 1 December 2016, <http://motherboard.vice.com/read/italian-cops-raid-surveillance-tech-company-area-selling-spy-gear-to-syria>
- ⁶⁴ "Network surveillance: Qosmos, a tool provider for Syria's leader al-Assad", Reuters, 9 May 2014, <https://reuters.com/network-surveillance-qosmos-a-tool-provider-for-syrias-leader-al-assad/>

As for middleman company AGT, it continues to operate, in part due to investment by Switzerland-based financiers. In April 2015, AGT attempted to broker the sale of intrusion software from Hacking Team to Egypt's military intelligence,⁶⁵ despite its poor reputation among industry peers⁶⁶ and Egypt's increasingly draconian treatment of journalists, opposition members and activists.⁶⁷

AGT has to date avoided scrutiny of its business dealings, which, as for many other surveillance middleman companies, have remained obscured even from the company's own staff. "I always had the feeling something is not right there," recalls one former employee. "I never really felt good about the business they did. But I never knew anything in detail. If you say [they were] selling surveillance, that would sound like them."

⁶⁵ "t: Military Intelligence Egypt", email from E Shehata to Aghiath Chbib, 9 April 2015, available at <https://wikileaks.org/hackingteam/emails/emailid/554337>. Accessed September 2015.

⁶⁶ "Re: Anas and Ayat from AGT [was: Fwd: MILIPOL Doha 2012]", email from Mostapha M. Aana to Hacking Team of cials, 15 October 2012, available at <https://wikileaks.org/hackingteam/emails/emailid/608555>. Accessed September 2016.

⁶⁷ "State repression in Egypt worst in decades, says activist", The Guardian, 24 January 2016, <http://www.theguardian.com/world/2016/jan/24/state-repression-egypt-worst-weve-ever-seen-activist-hossam-bahgat>.

Conclusion

The Syrian government built a surveillance state using Western technology provided by companies and their middlemen at a time when the abuses of the government would have been well known to even the most casual observer. Certain of the surveillance technology suppliers seem happy to have turned a blind eye, or at least not to have sought to know, the conduct of their intermediaries and of the end-users of their products. AGT, as an intermediary, managed to profit from questionable sales to governments, such as to the Syrian government and Libyan government under Colonel Gaddafi, that were publicly engaged in repression.

Privacy International recommends that governments and their relevant authorities:

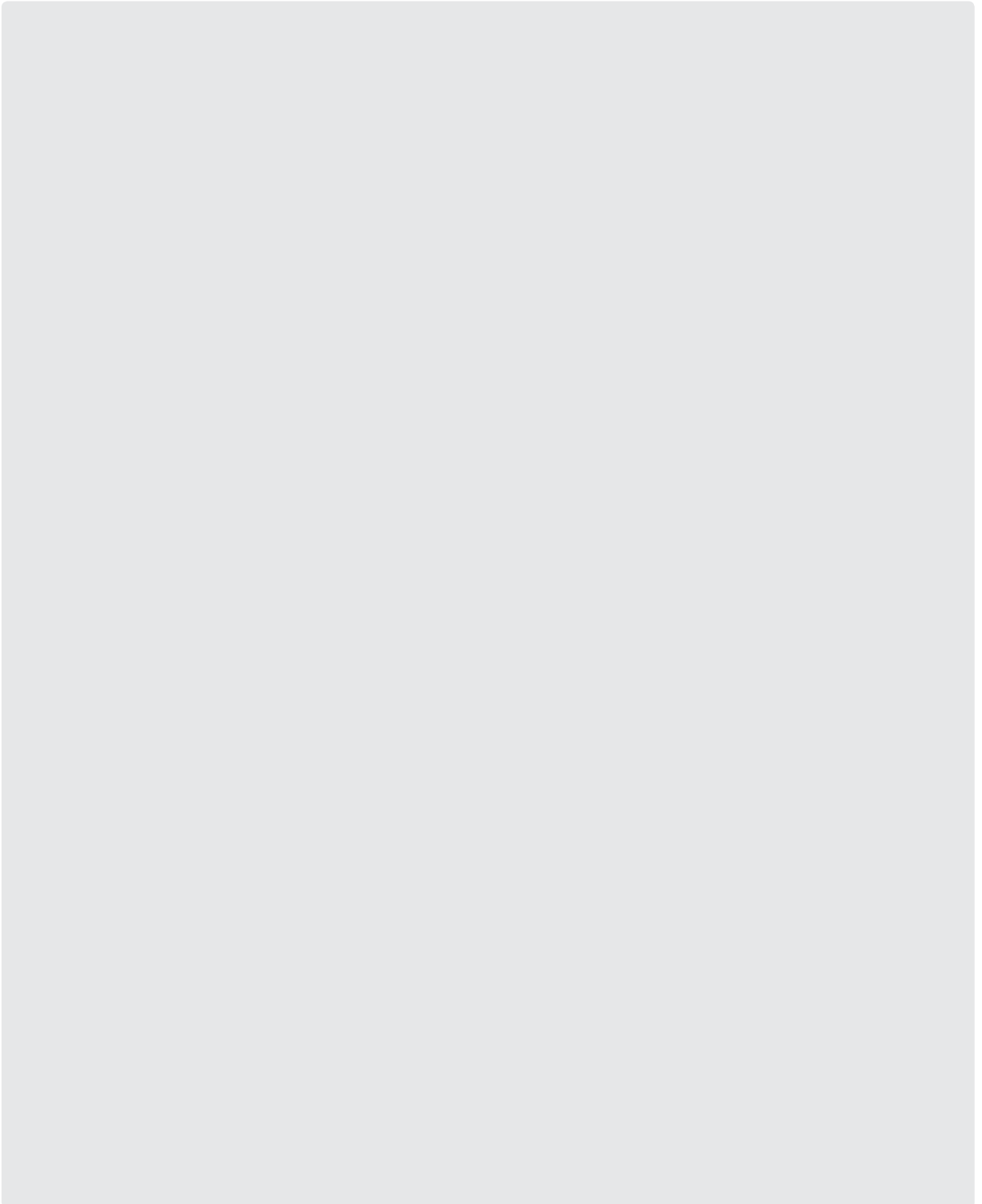
- Ensure that all relevant surveillance technologies are subject to a licencing regime, which is reviewed on a regular basis. Develop a policy mechanism to efficiently identify products that can be subjected to export licencing with sufficient input from a range of stakeholders, including independent technical experts, academics, and civil society. Particular attention should be paid to ensuring that the inclusion of any technology does not harm security research or otherwise negatively impact the development of the information and communications technology sector.
- Work within existing 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 issues.
- Ensure human rights criteria are included in export control assessment procedures that are specific to surveillance technologies. Export licences should be denied where there is a risk the surveillance technologies will be used to facilitate internal repression or to otherwise undermine human rights, or if there is no clear legal framework governing their use. Human rights criteria should take into account the human rights record of the end user of the technology, the potential for the technology to be used in a manner not compliant with international human rights standards, the legal framework to regulate the use of the technology by the end user and oversight mechanisms.
- Require companies exporting surveillance technologies to provide clear end-use assurances from their customers in contractual agreements. Those assurances must encompass human rights safeguards and protect against the arbitrary and unlawful use of surveillance technologies.
- Ensure that data about licencing decisions is available to legislative bodies and the public to allow scrutiny and accountability for decisions and to provide information about the surveillance trade. This data should contain the category of license applied for, the category of equipment applied for, details concerning the exporter, details concerning the end-user, the total cost of license applied for, the destination of the export for which the license has been applied for, and the decision by the licencing authority concerning the application.

Privacy International recommends that companies selling surveillance technologies:

- Ensure they have a functioning compliance regime to mitigate against sanctions and export control violations.
- Carry out due diligence research on any potential beneficial end-users prior to agreeing to a transaction.
- Not sell or provide a surveillance product if the potential beneficial end-users of the product cannot be clearly identified or has a documented record of human rights abuse that is likely to be enabled by the product.
- Not sell or provide a surveillance product to a customer if there is no clear legal framework or oversight mechanism governing use of the product within the destination country.
- Stipulate clear end-use assurances in contractual agreements with customers encompassing human rights safeguards and protecting against the arbitrary and unlawful use of the surveillance product.
- Carry out a periodic review of the sale or provision of surveillance products and refuse to carry out maintenance, training, or updates if the end-user does not conform to contractual obligations, including end-use assurances.
- Develop internal policies relating to re-sellers and distributors, and include provisions in contractual agreements with these entities ensuring their adherence to sanctions and export control regulations and to the developer's own human rights provisions.
- Original Equipment Manufacturers (OEMs) should ensure that the company incorporating their equipment adheres to export control regulations and to the OEM's own human rights provisions.
- Commit to and publish strong Corporate Social Responsibility (CSR) commitments conforming to the United Nations' Guiding Principles on Business and Human Rights' in relation to 'human rights'.
- Initiate an annual review of adherence to CSR commitments and international human rights standards and publish its outcomes. Included within this should be strong transparency measures containing, to the greatest extent possible, a list of end-users.

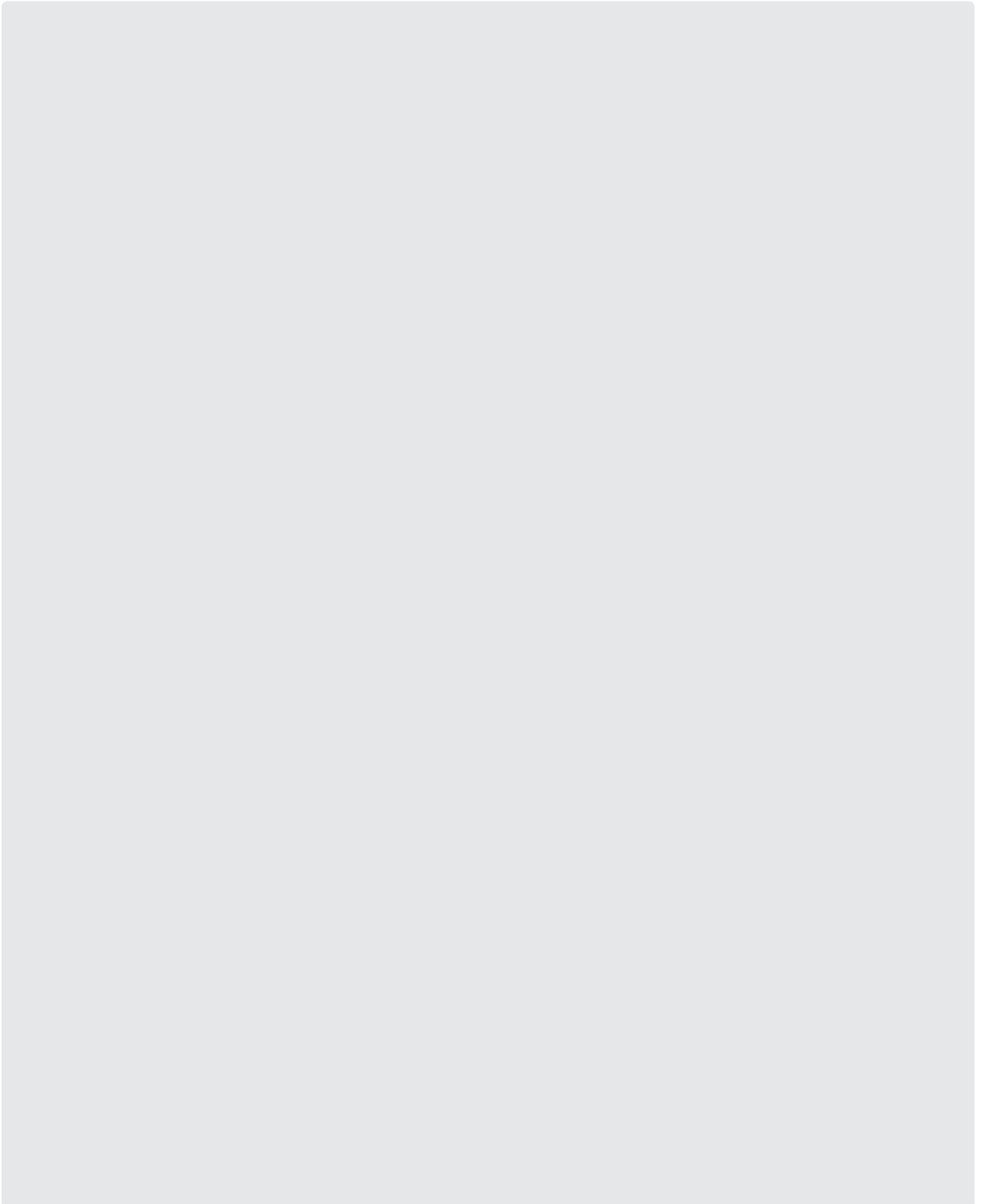
Annex 1

Excerpt from STE call for tenders for a Central Monitoring System, October 2007



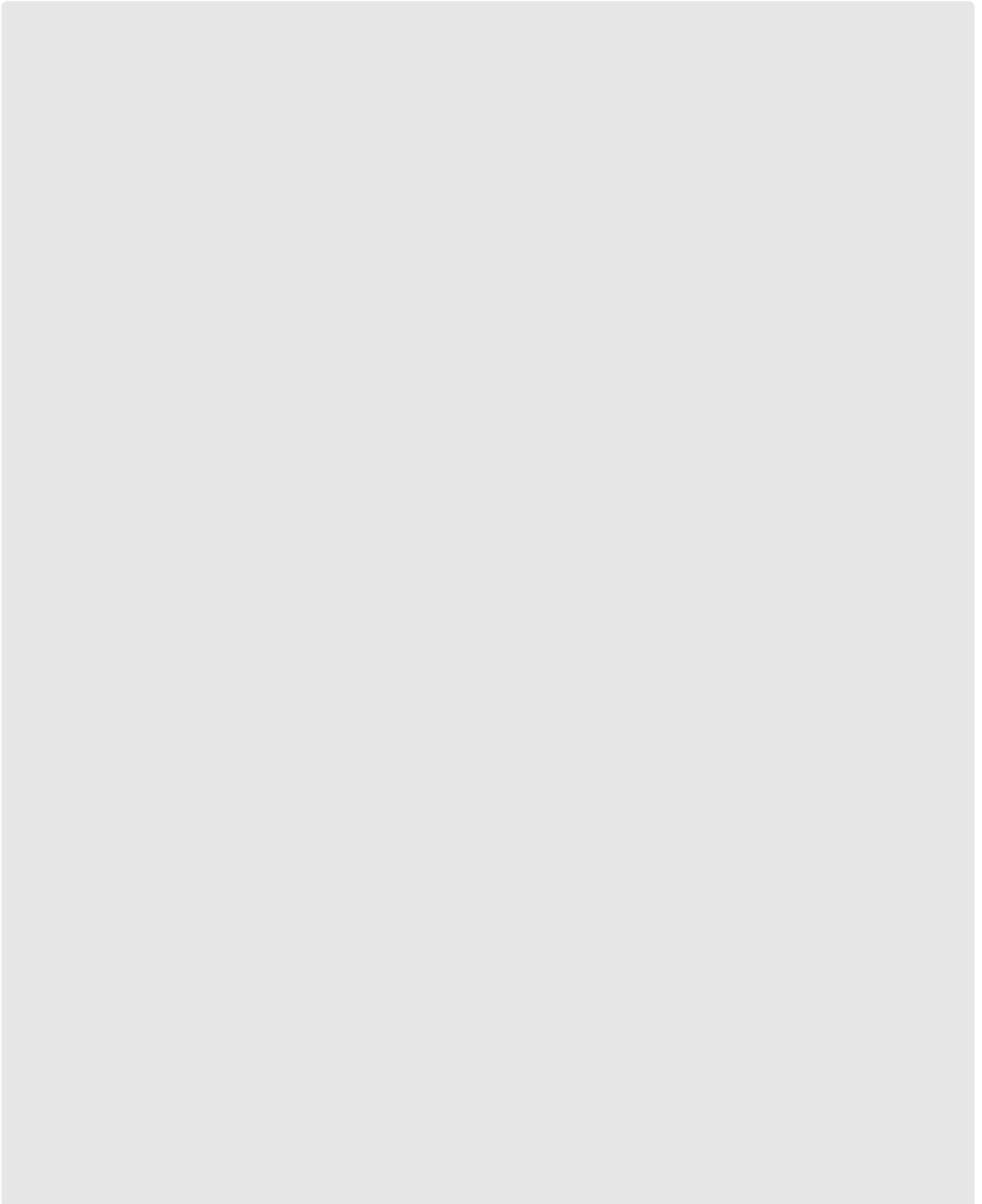
Annex 1 continued

Excerpt from STE call for tenders for a Central Monitoring System, October 2007



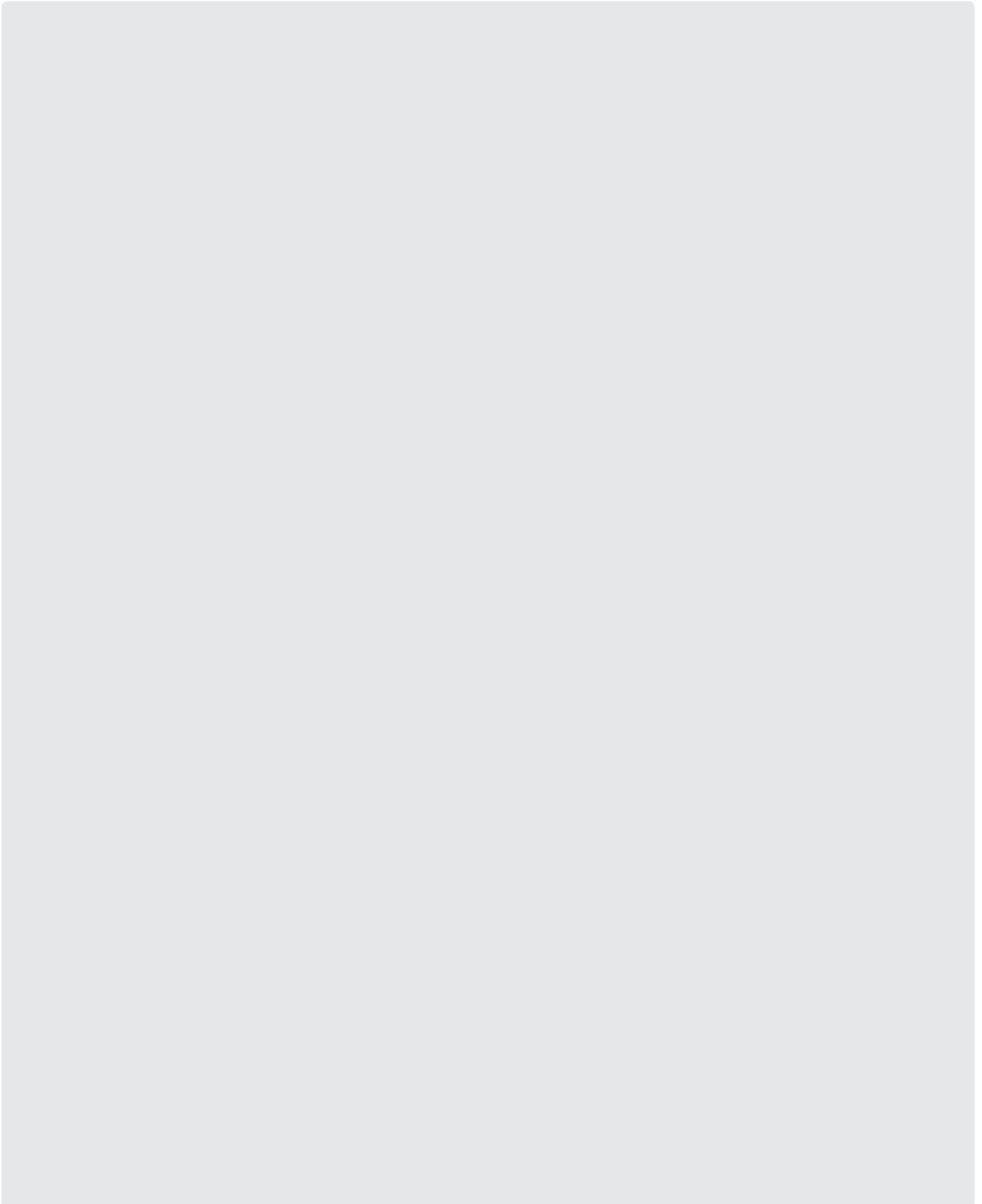
Annex 1 continued

Excerpt from STE call for tenders for a Central Monitoring System, October 2007



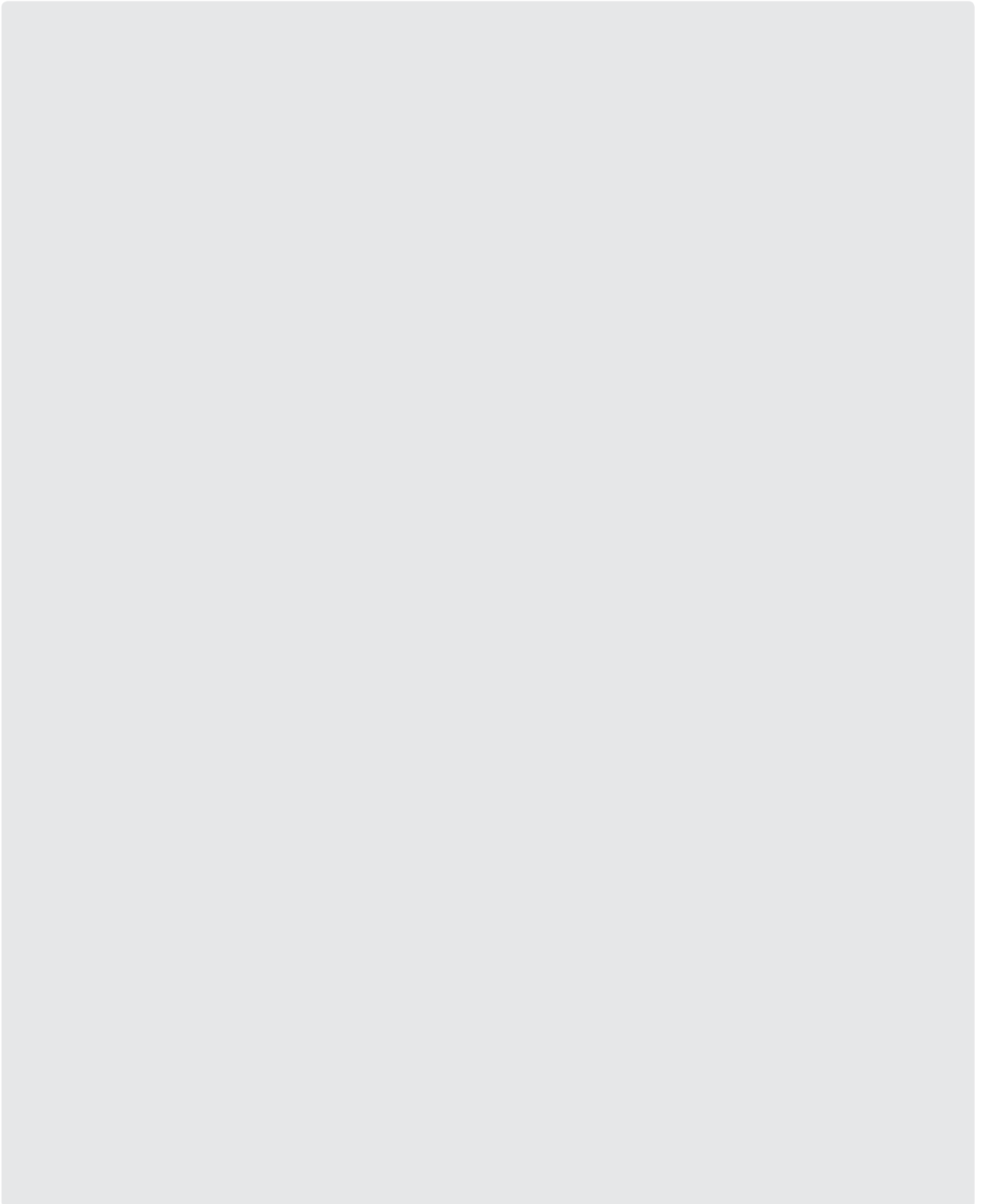
Annex 1 continued

Excerpt from STE call for tenders for a Central Monitoring System, October 2007



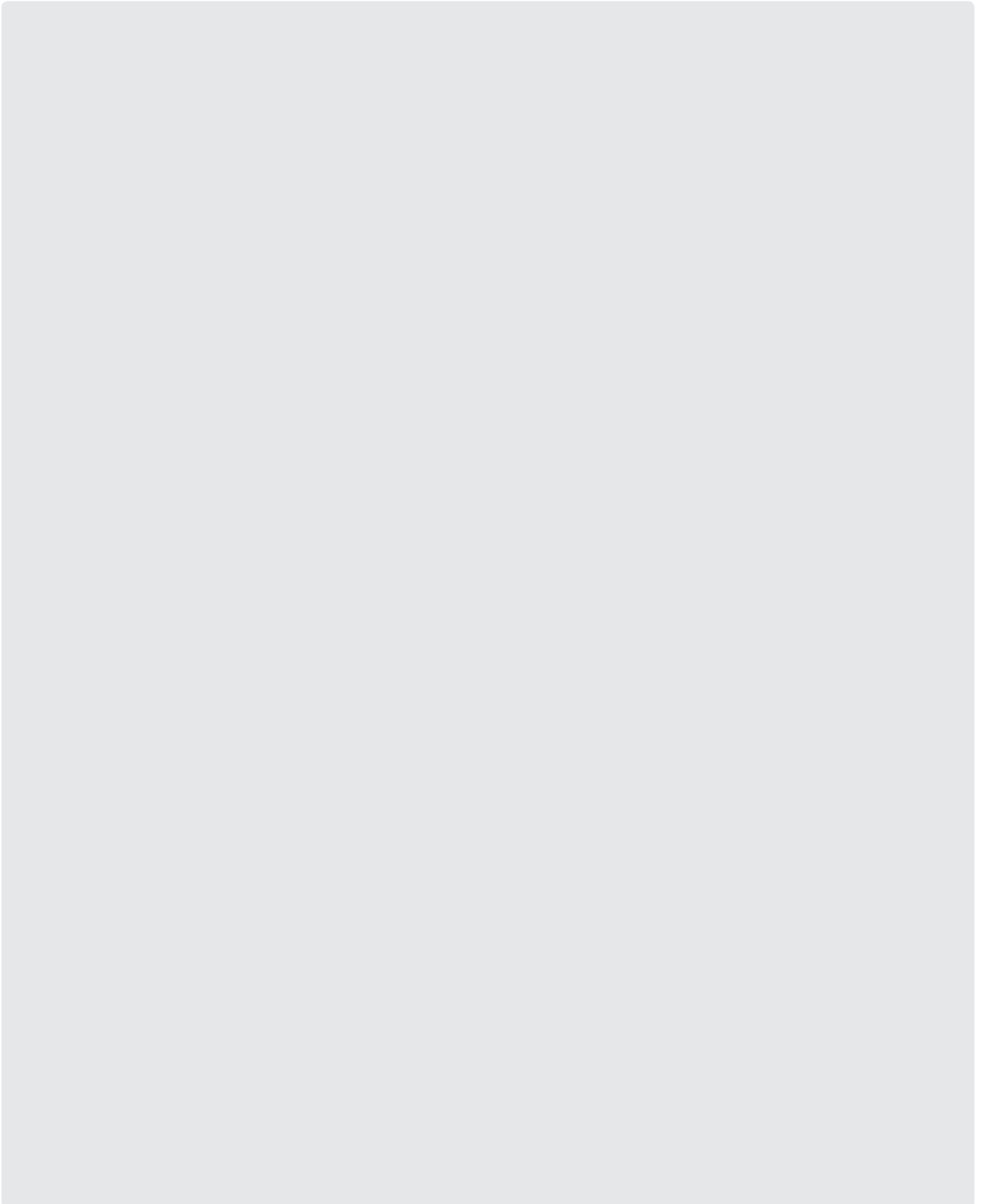
Annex 1 continued

Excerpt from STE call for tenders for a Central Monitoring System, October 2007



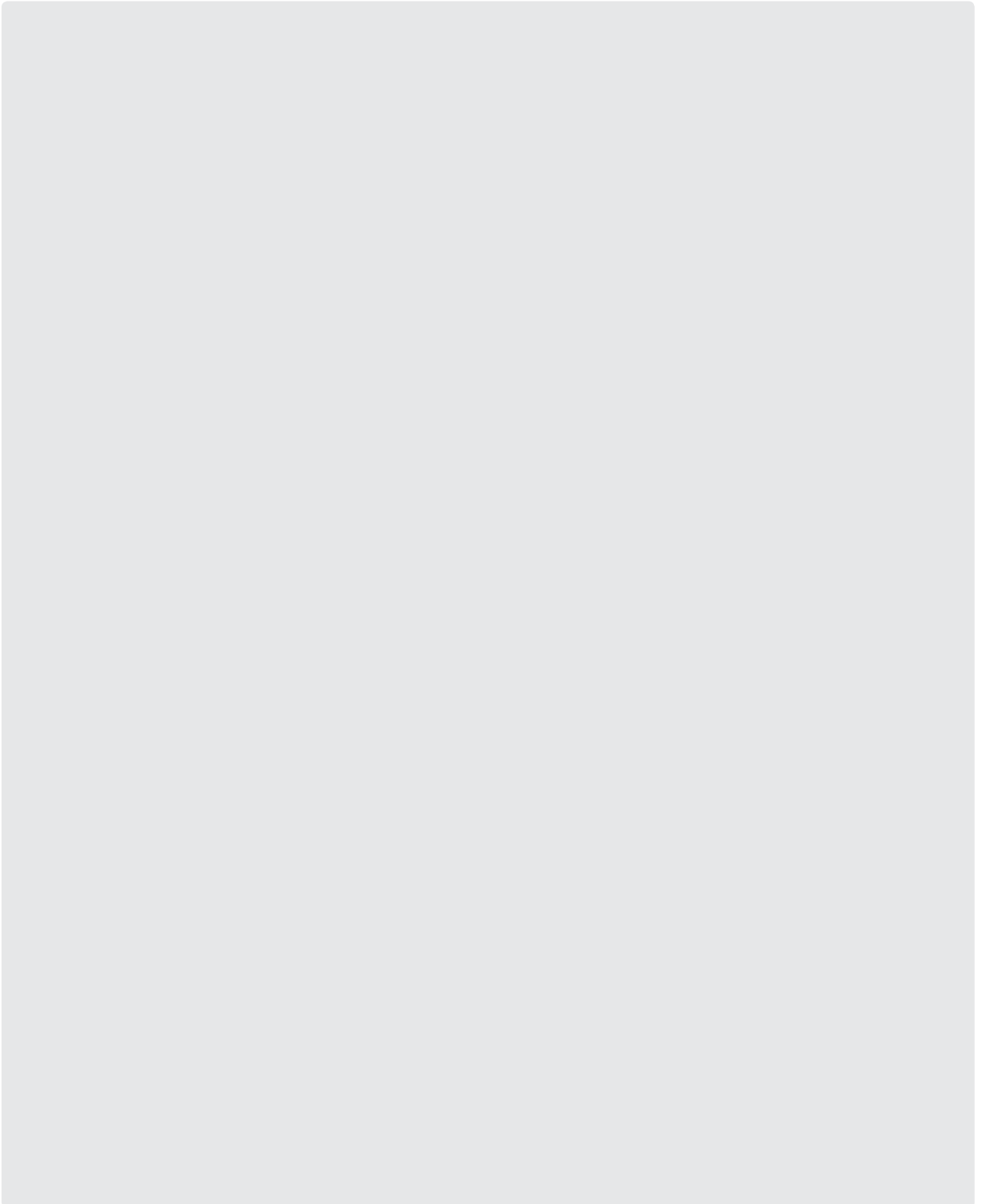
Annex 2

Excerpt from STE requirements for Content Filtering project, April 20 09



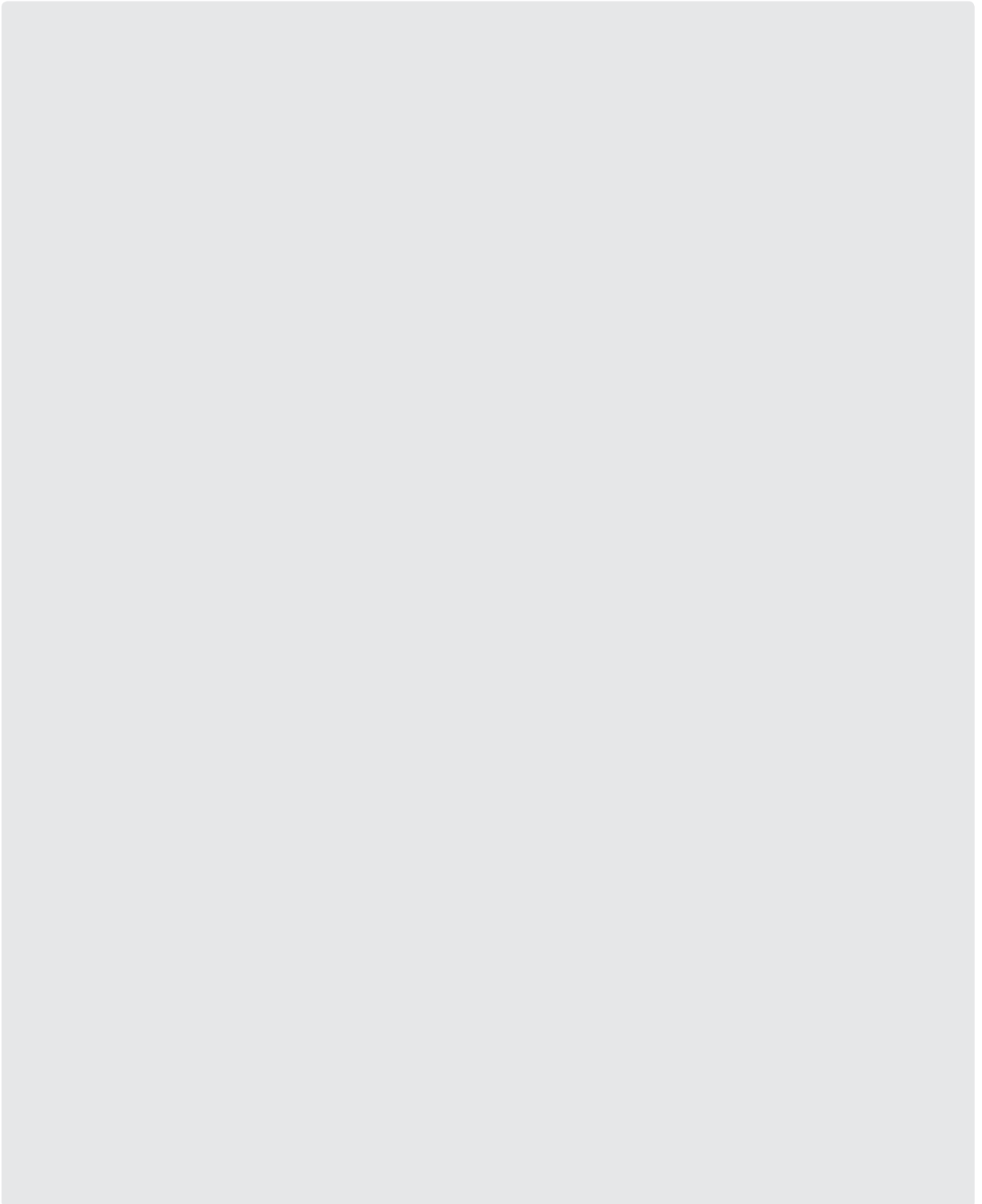
Annex 2 continued

Excerpt from STE requirements for Content Filtering project, April 20 09



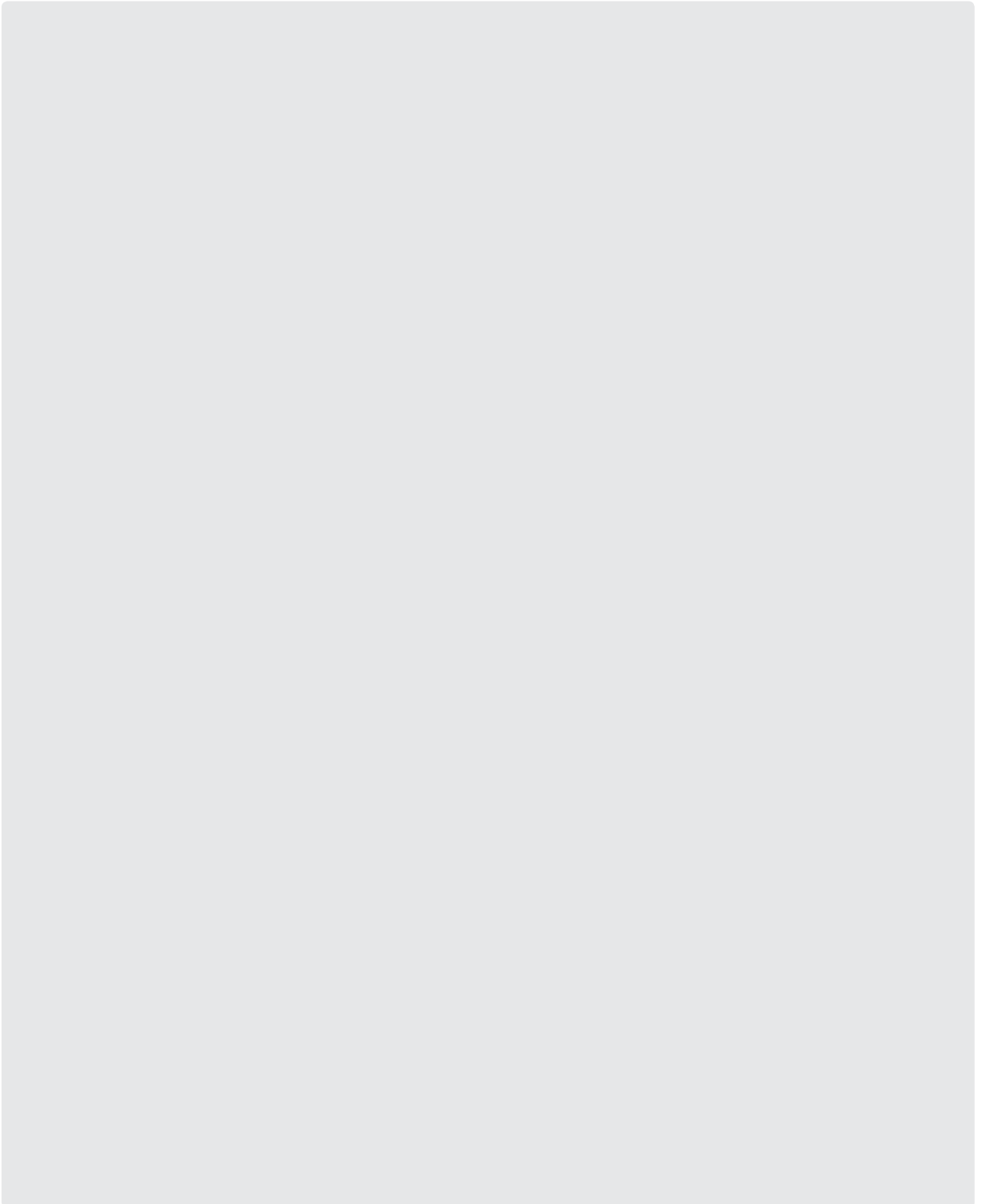
Annex 2 continued

Excerpt from STE requirements for Content Filtering project, April 20 09



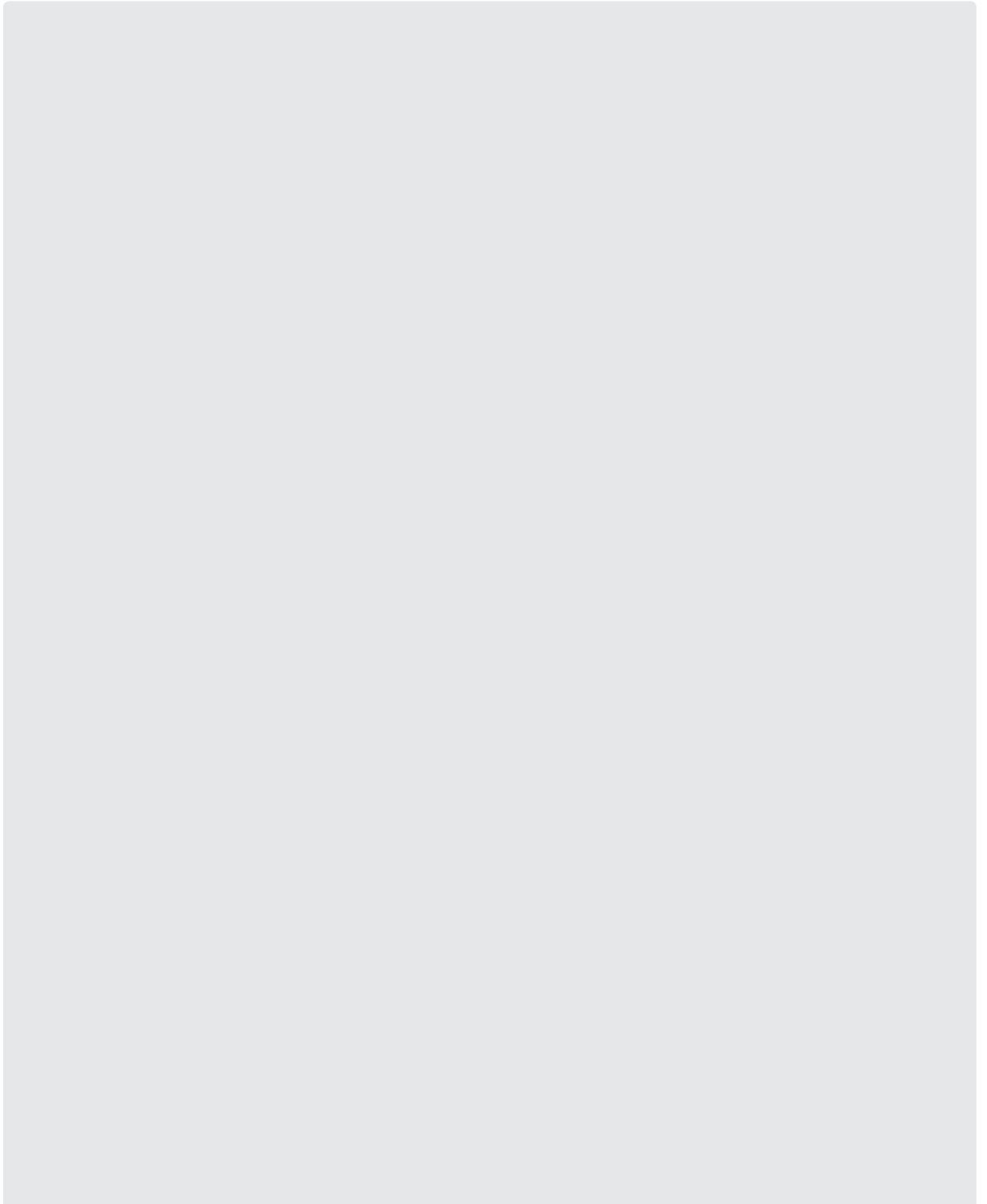
Annex 3

Letter from AGT to STE asking to be reconsidered for Central Monitoring System project, November 2009



Annex 3 continued

Letter from AGT to STE asking to be reconsidered for Central Monitoring System project, November 2009



Annex 4

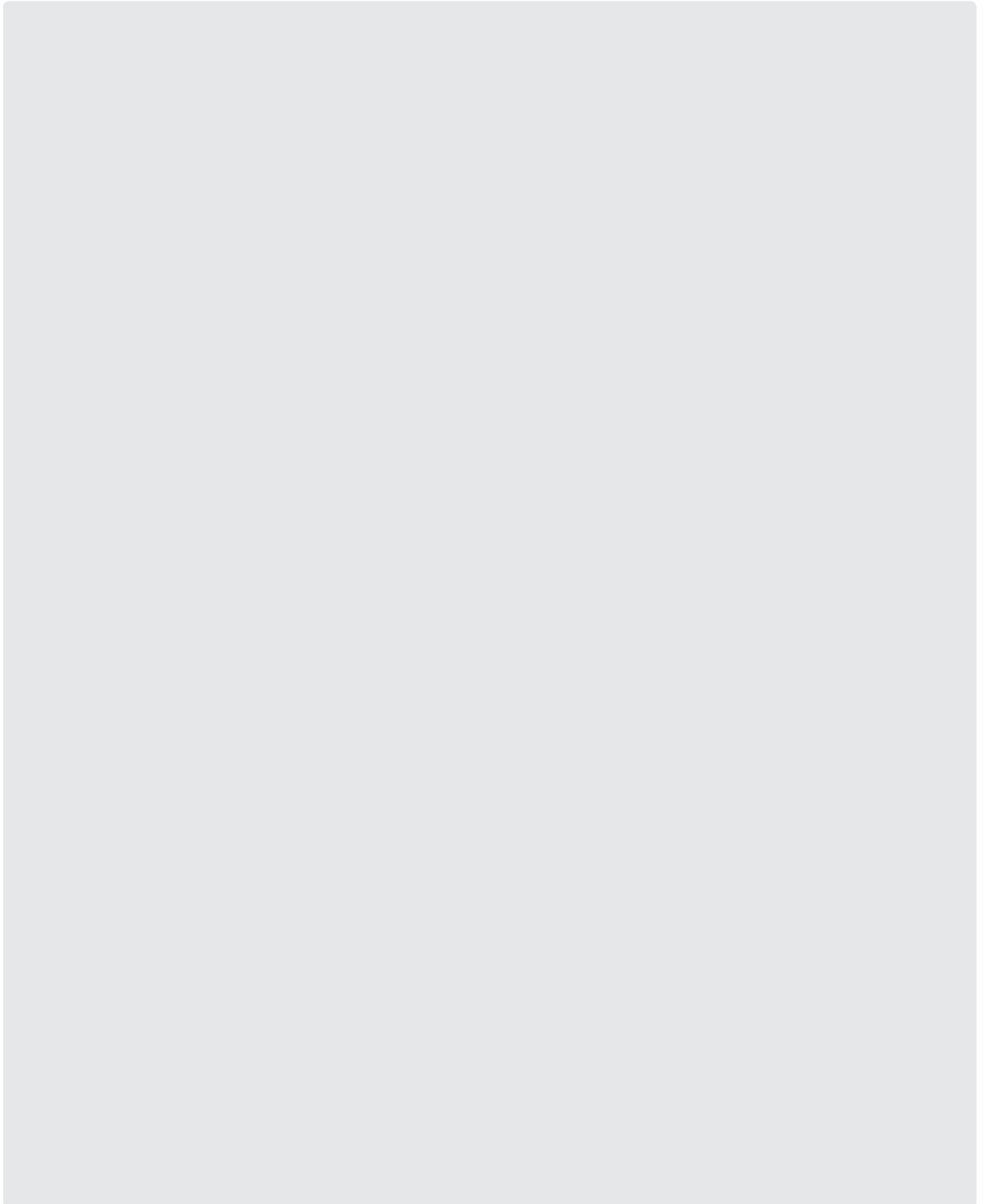
Excerpt of AGT-VASTech proposal for brute force voice identification of phone users in Syria, July 2009

**Evaluation of the practicality of brute force
Speaker Identification in massive sets of
calls**

**Proposal of an alternative approach that is
more practical and provides an improved
benefit:cost ratio**

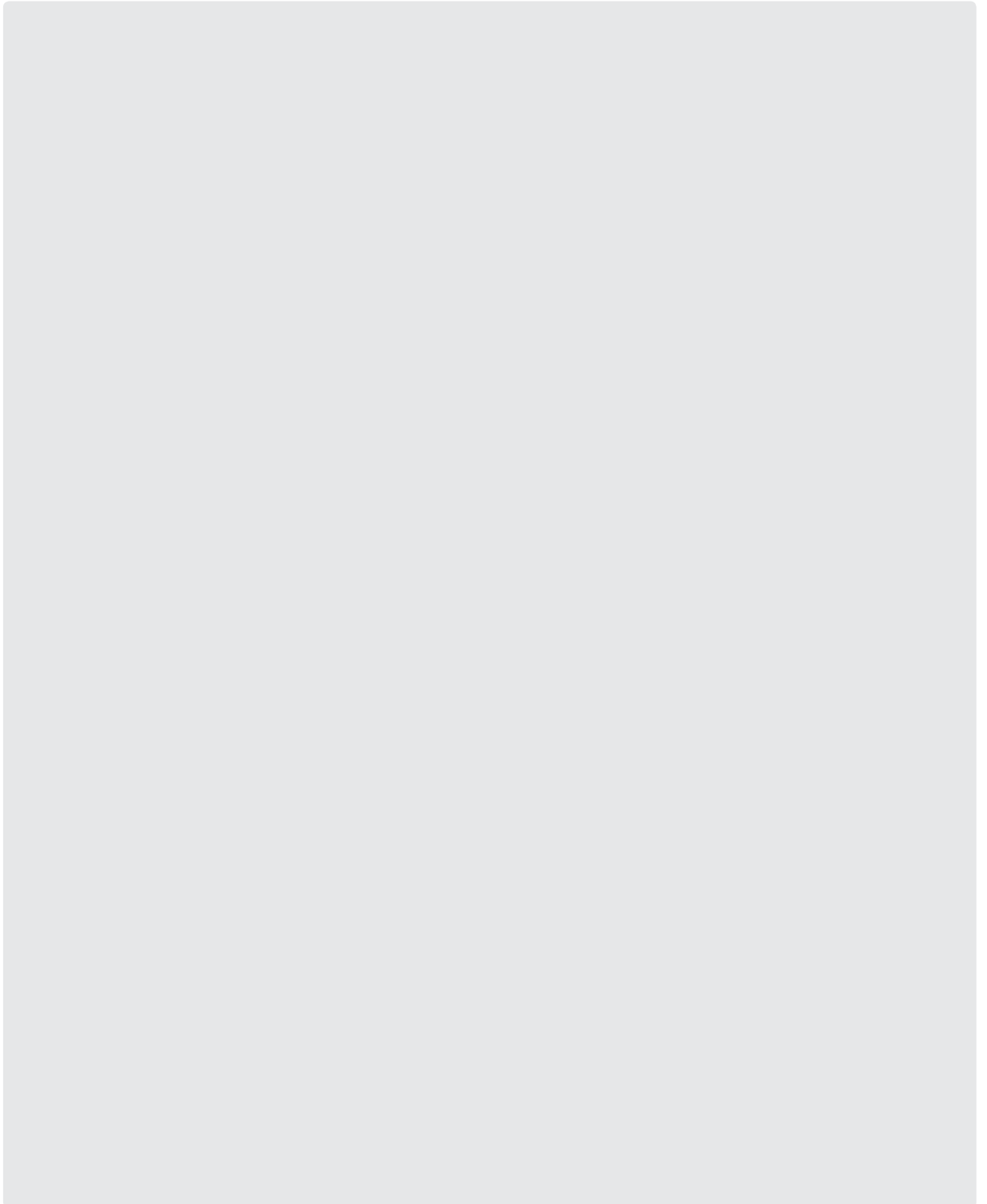
Annex 5

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



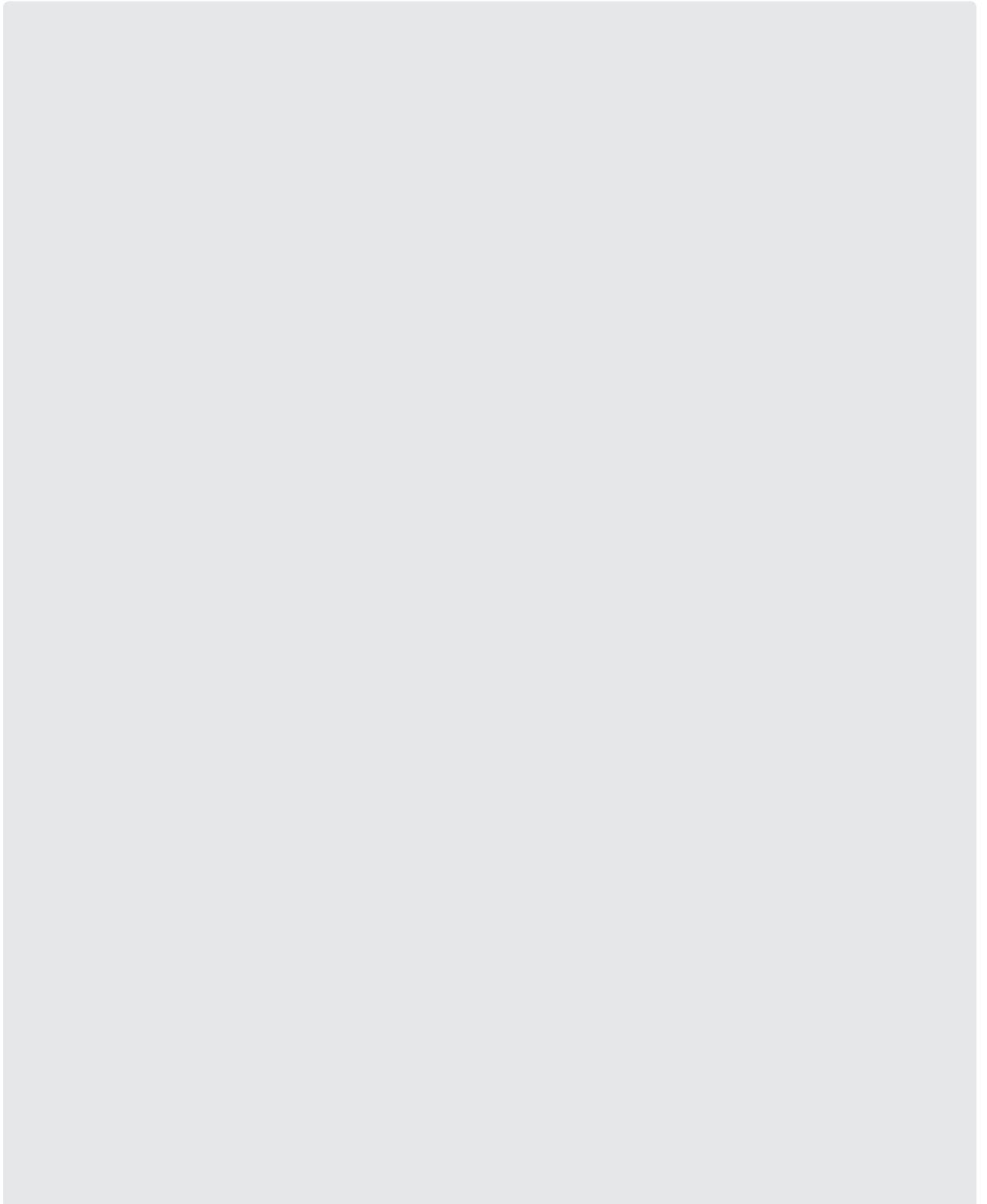
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



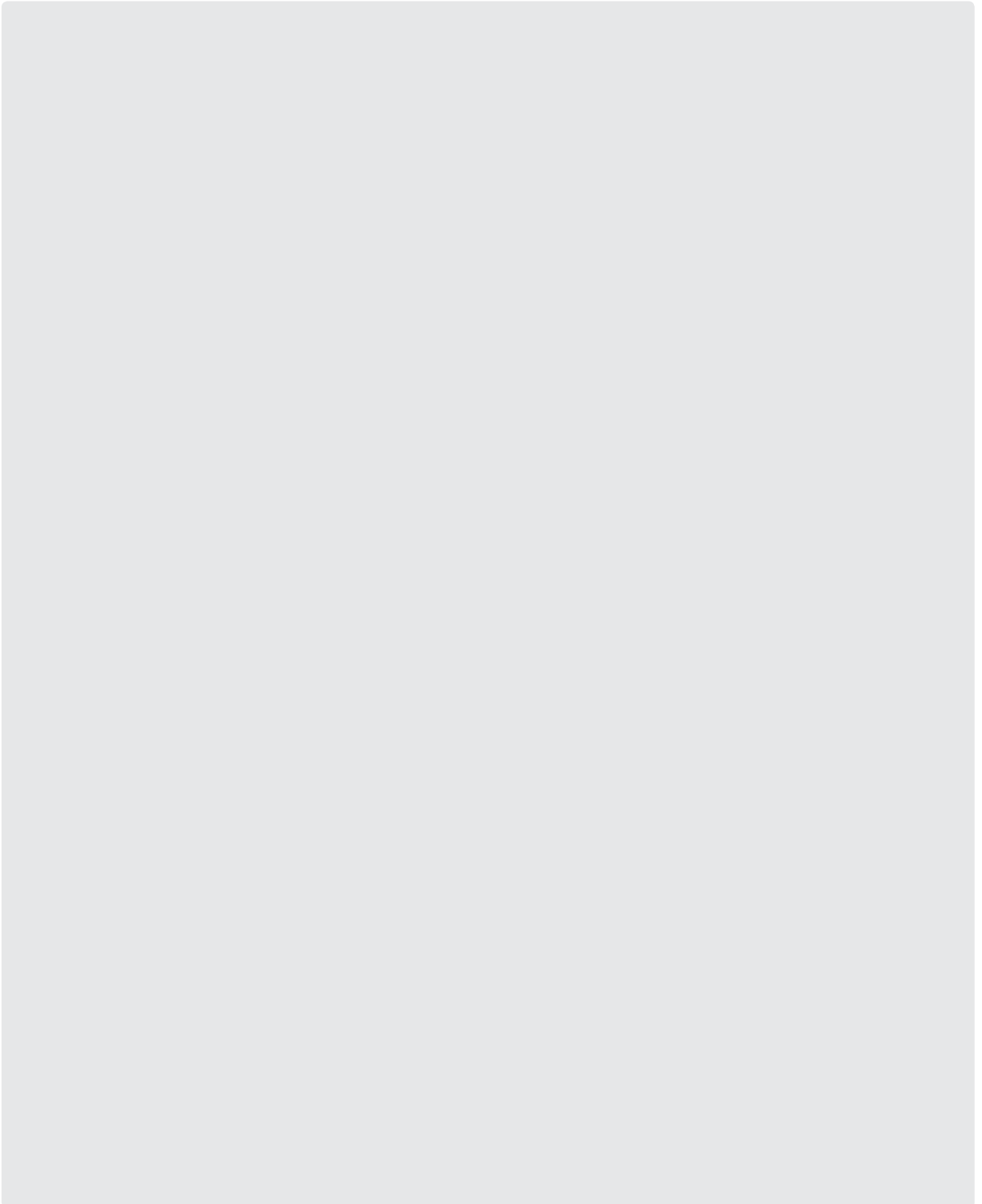
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



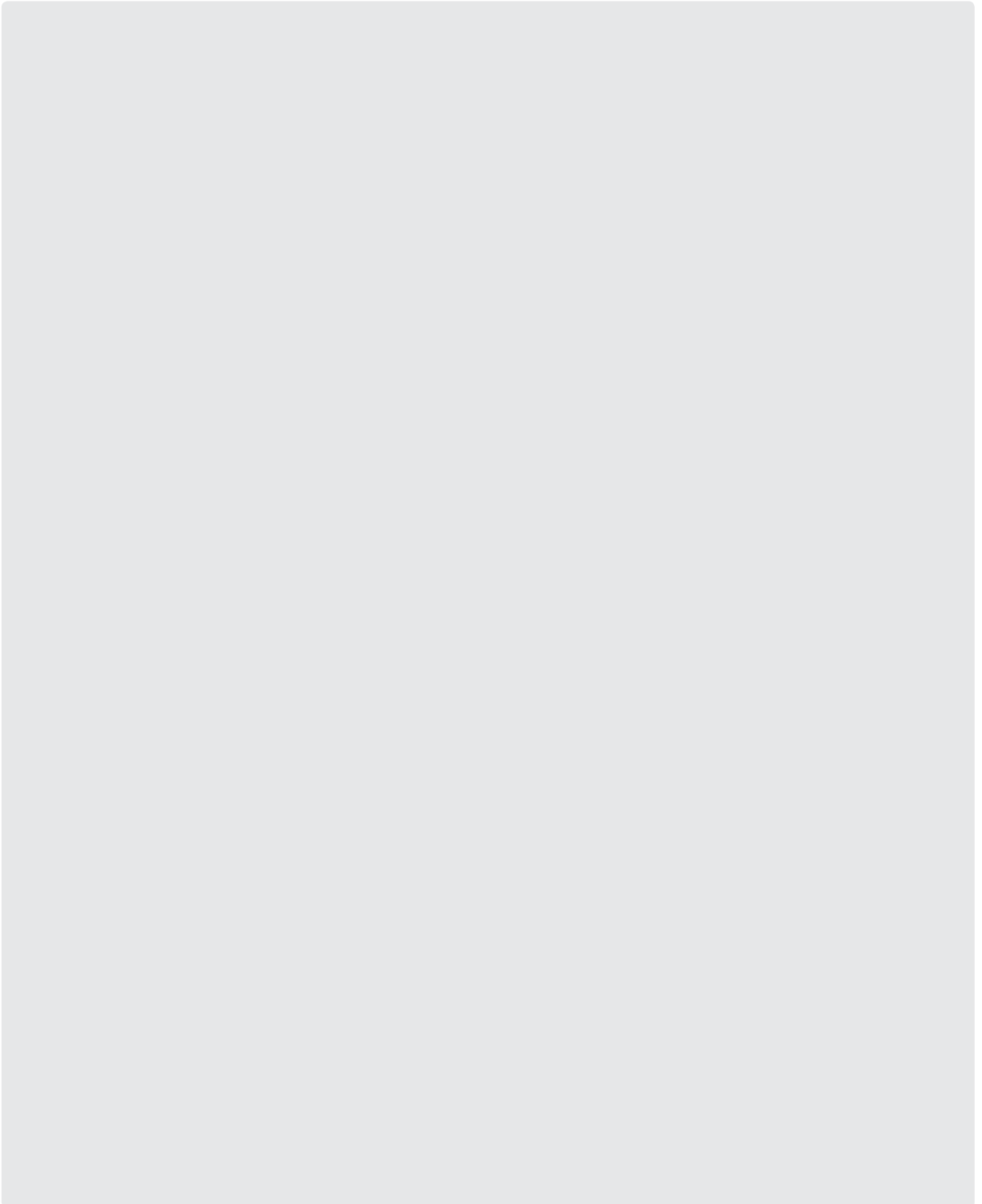
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



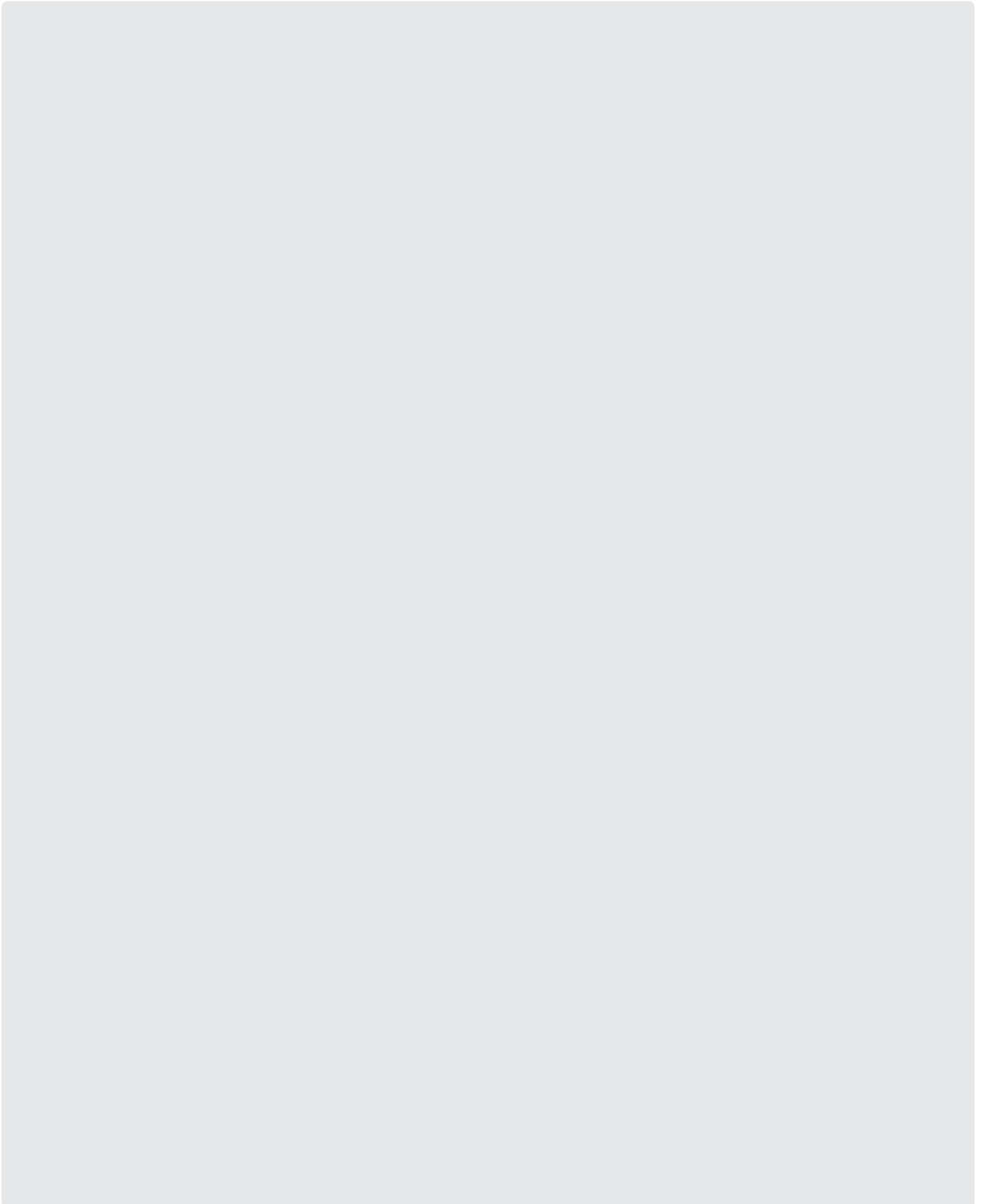
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



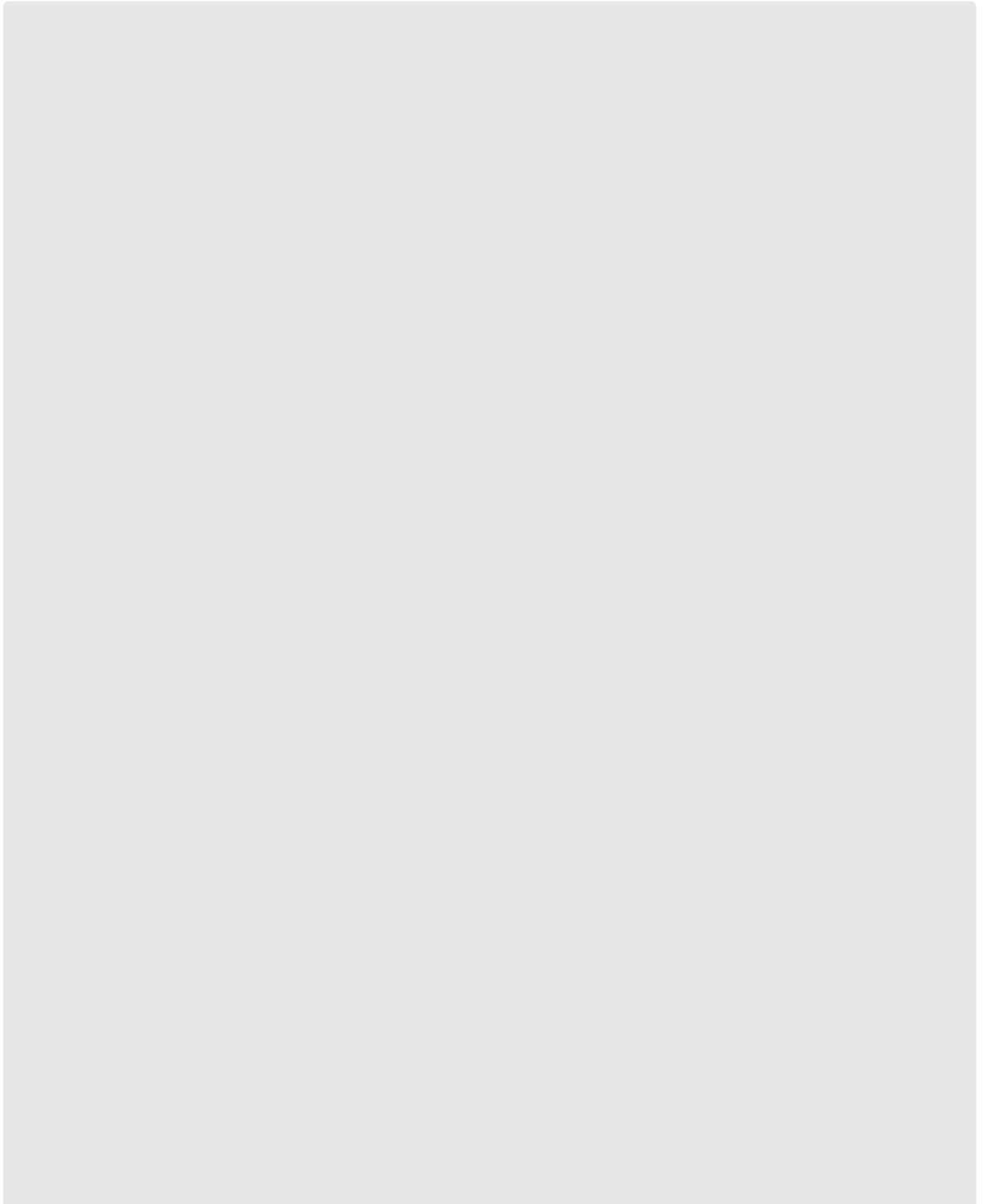
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



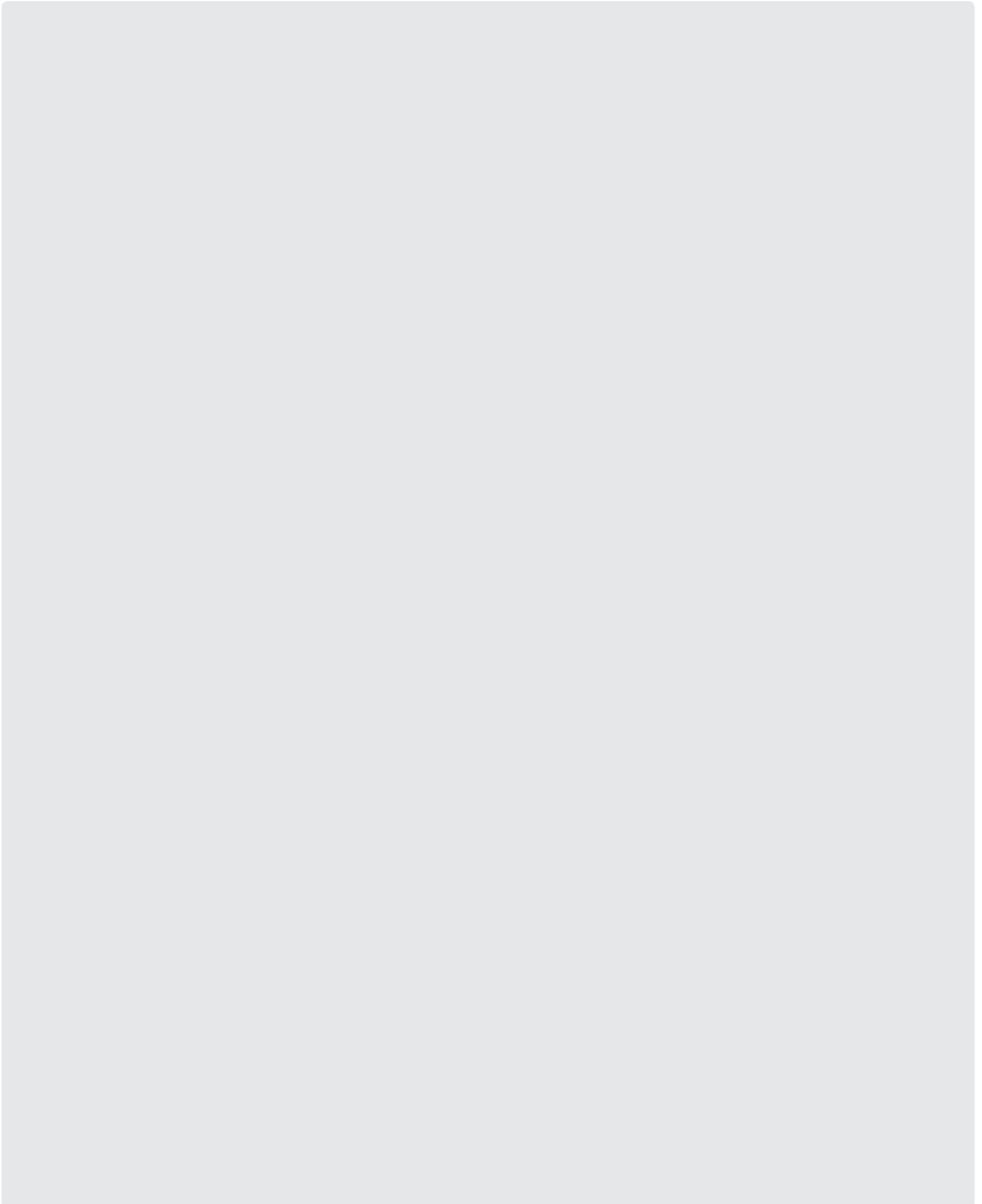
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



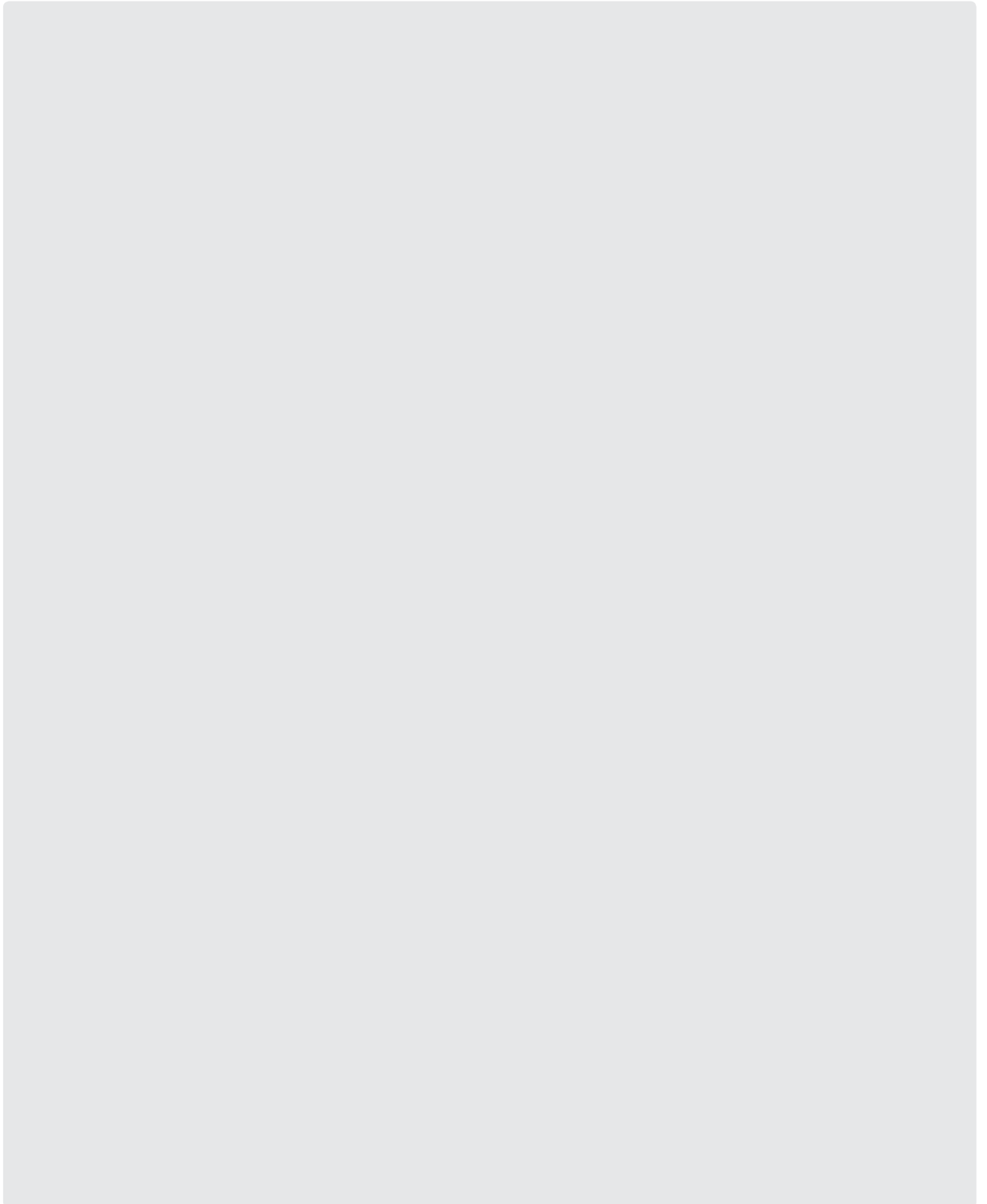
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



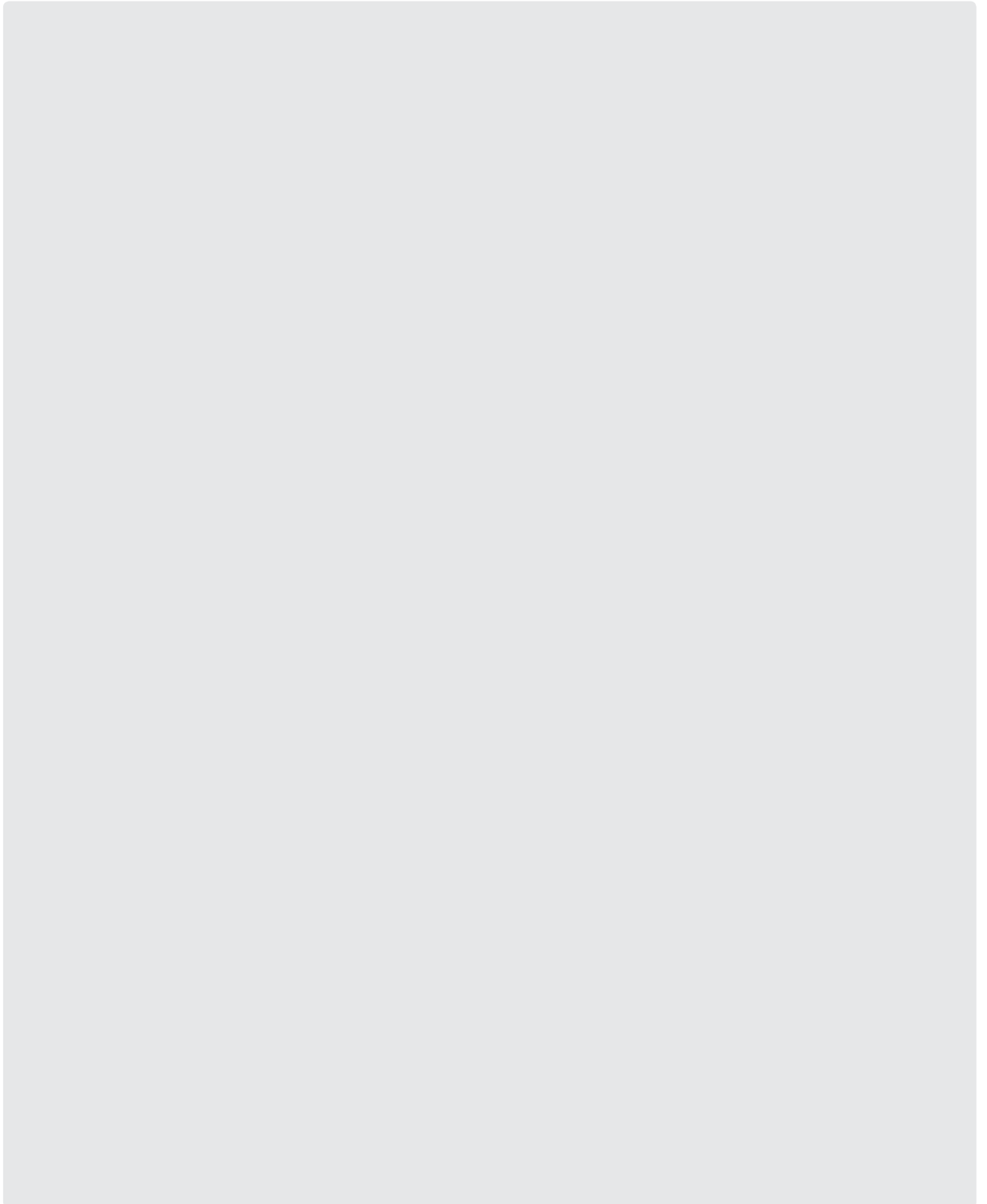
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



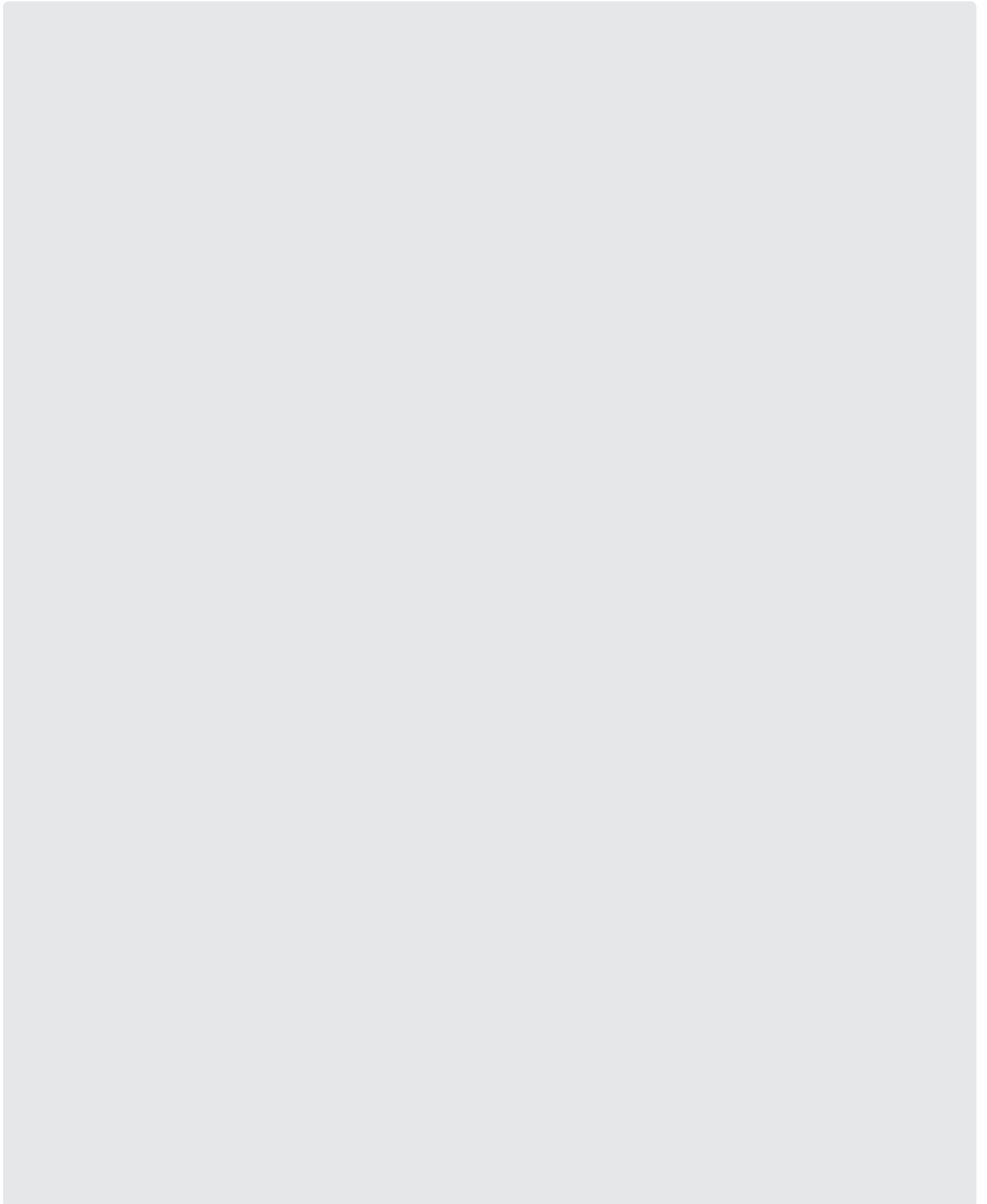
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



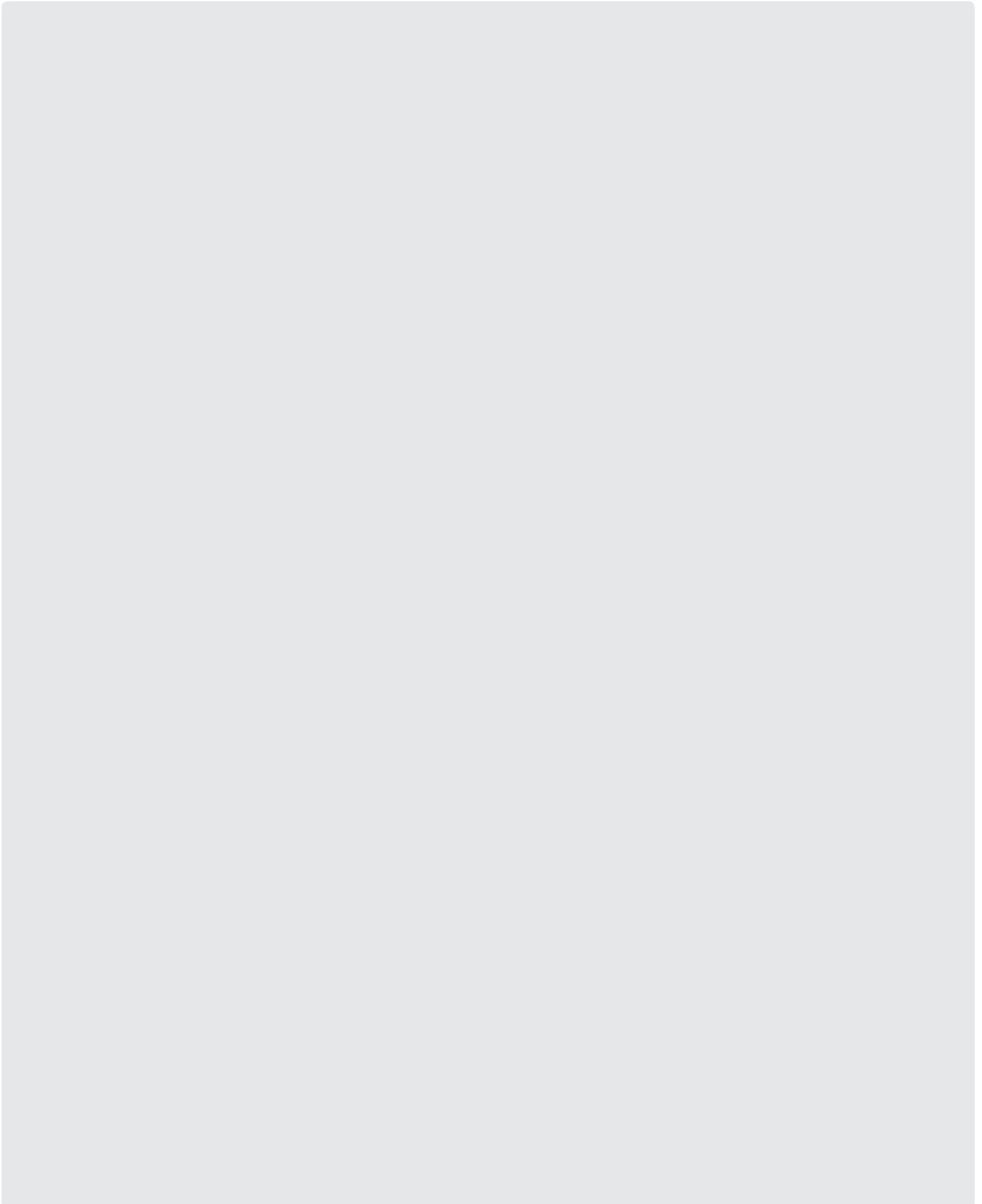
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



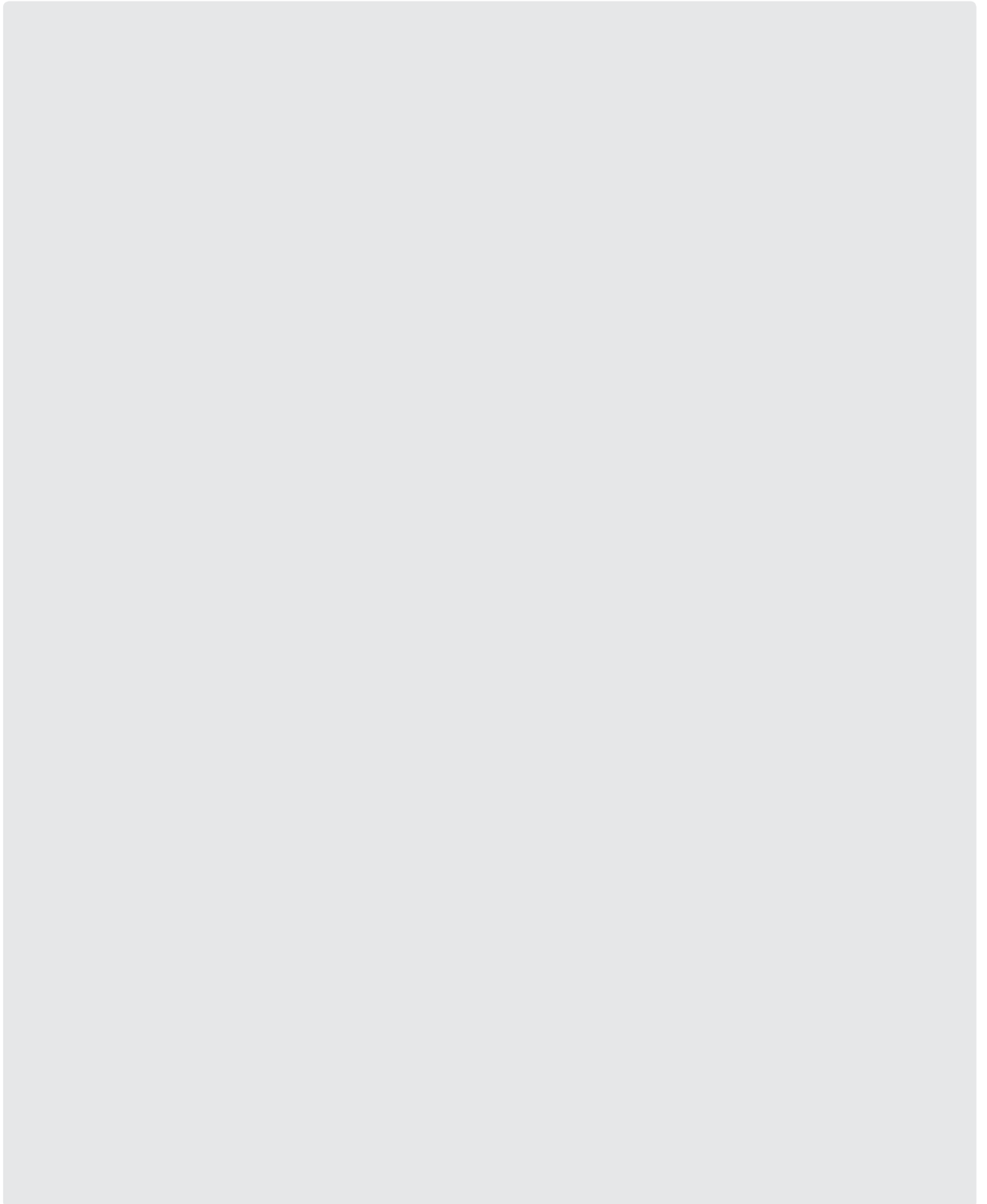
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



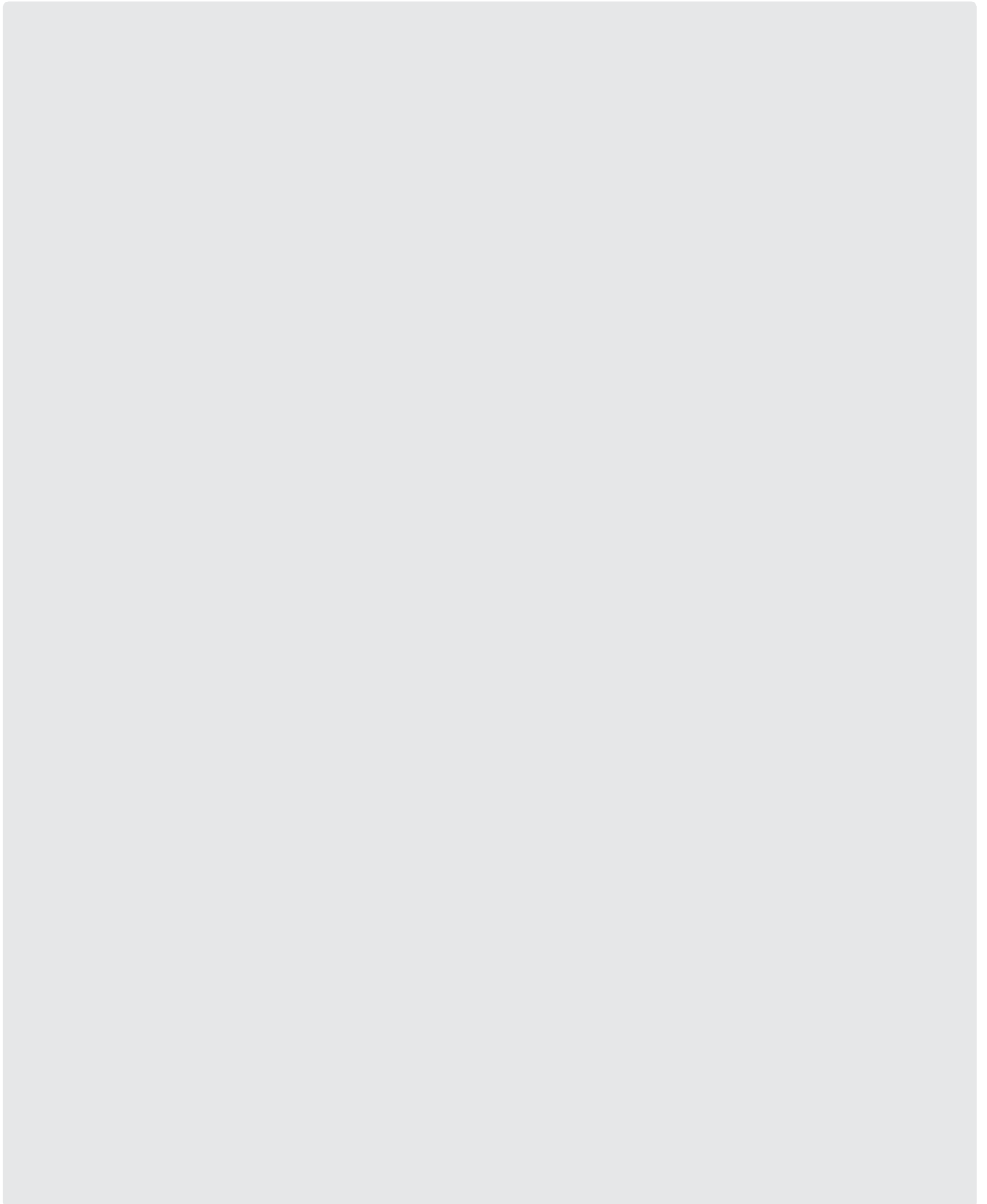
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



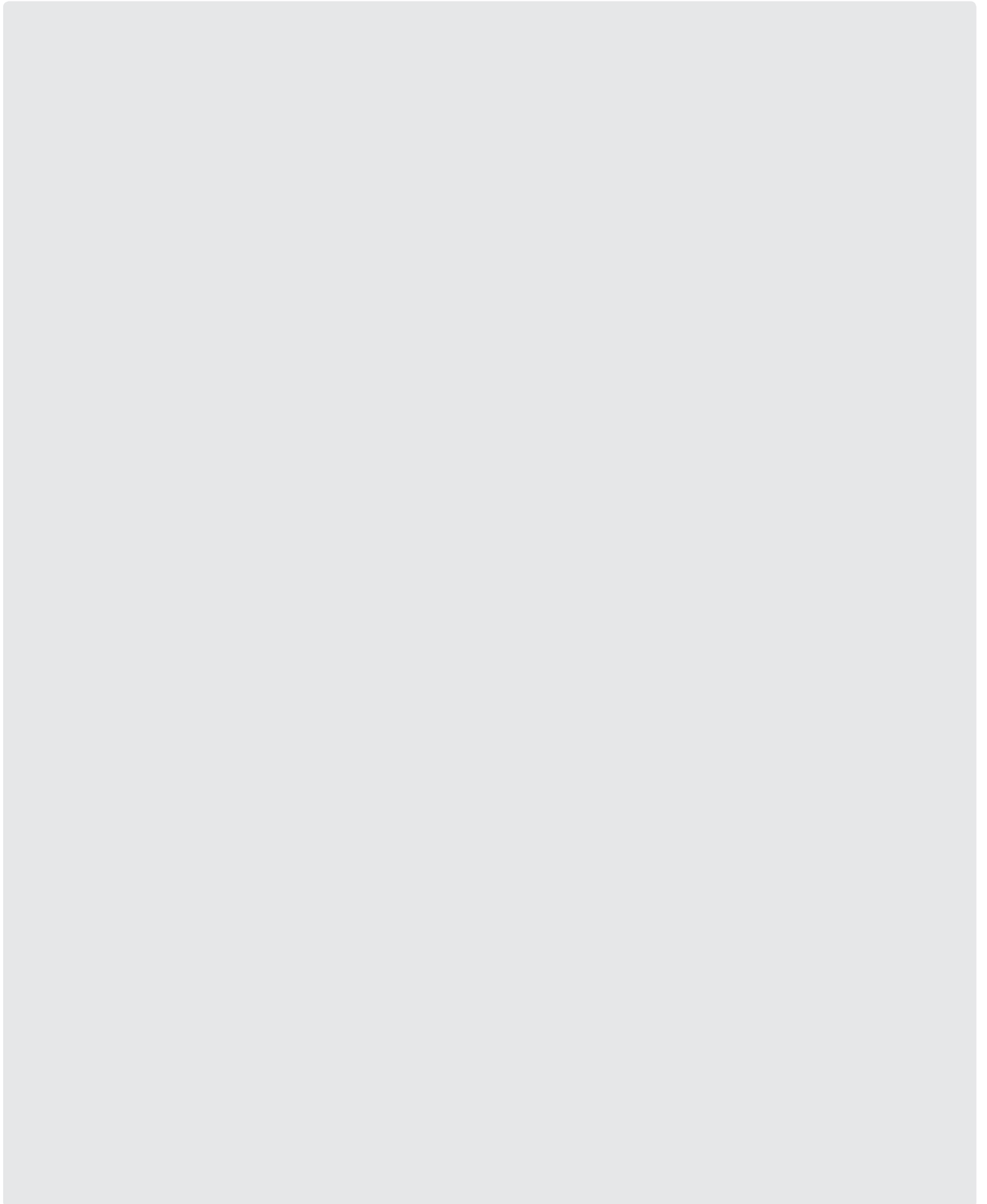
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



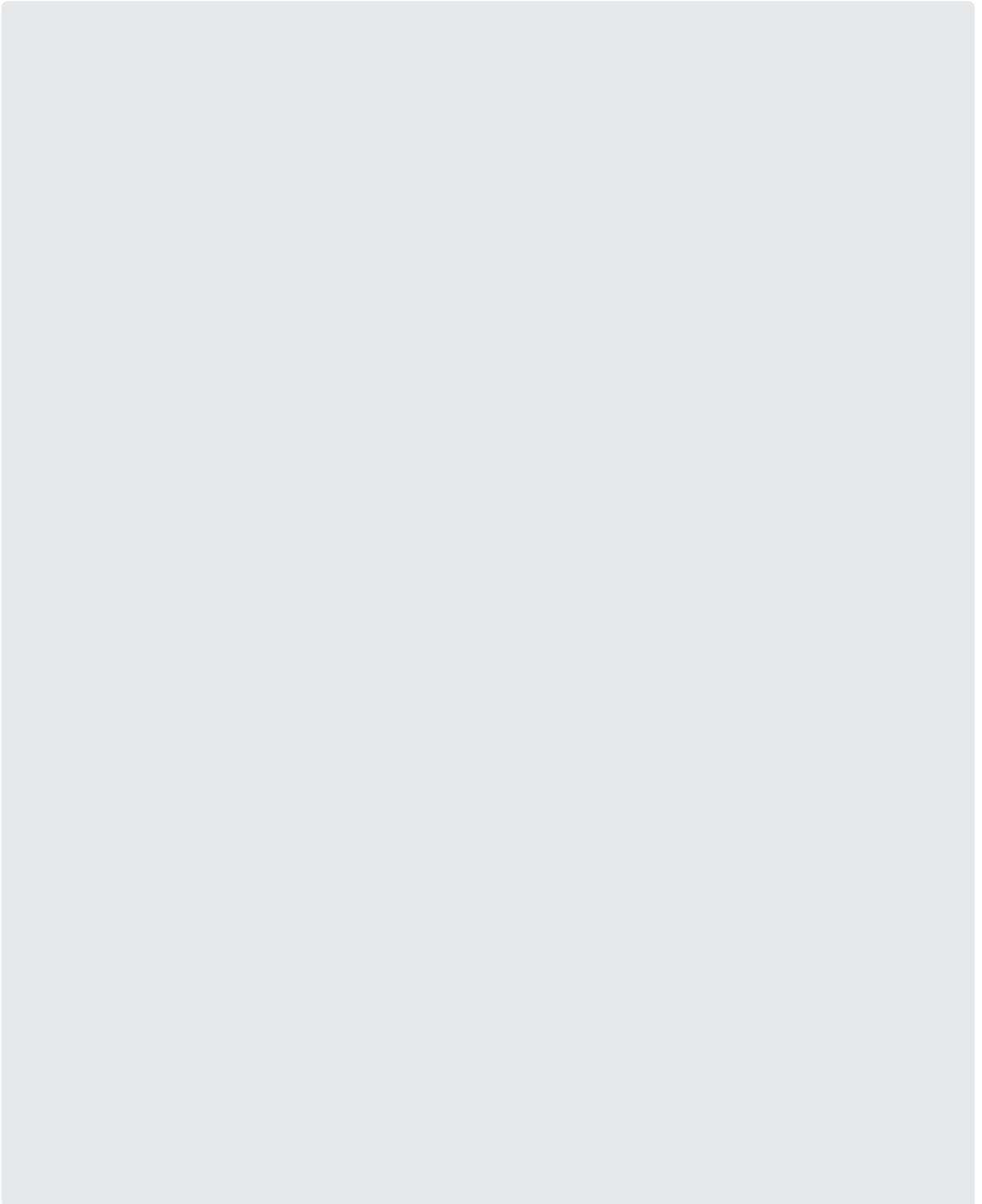
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



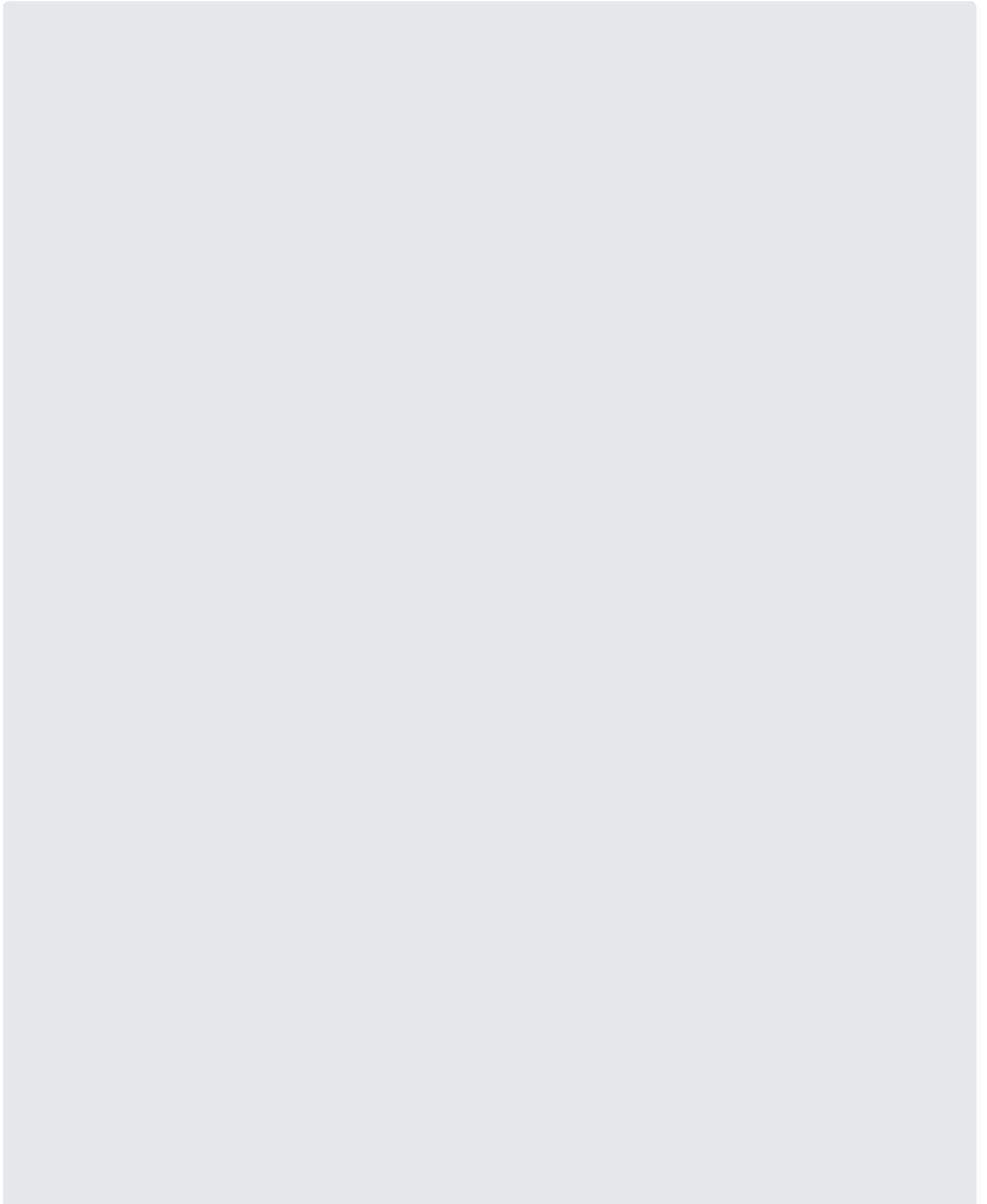
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



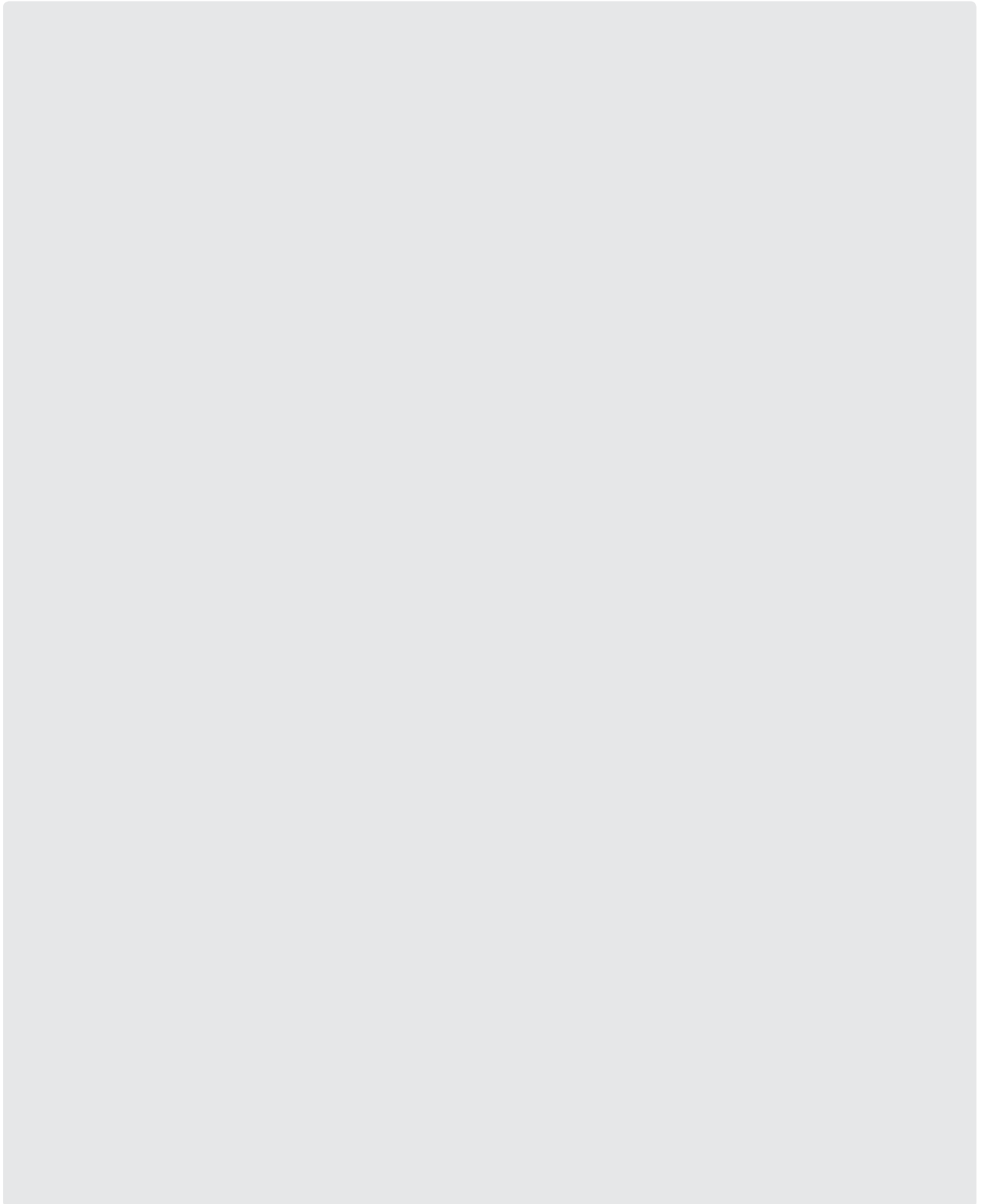
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



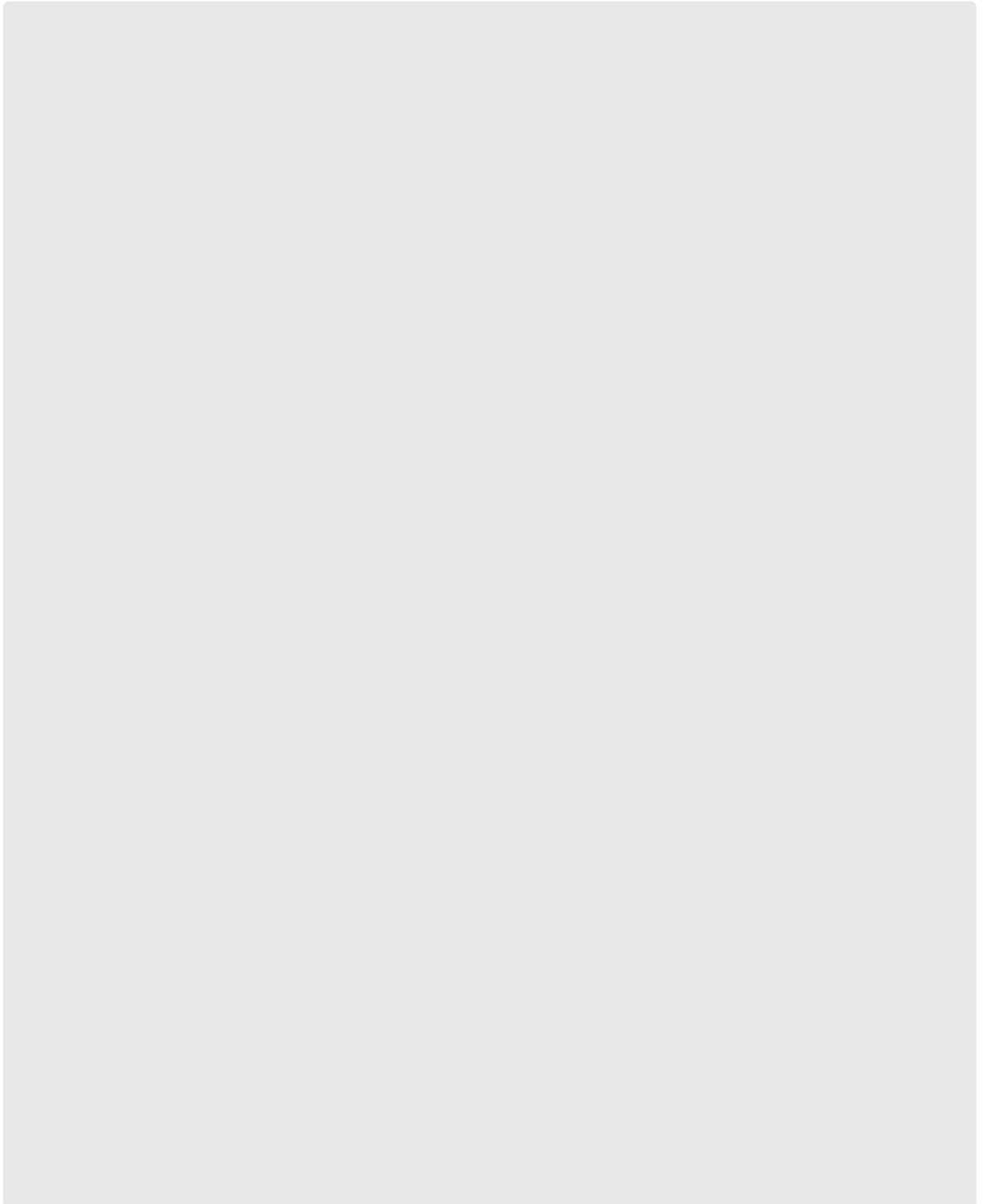
Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



Annex 5 continued

Technical proposal from RCS/AGT to SCT for Satellite ISP interception, August 2009



Annex 6

Response from AGT, December 2016.

From: Anas Chbib [AGT] <achbib@agt-technology.com>
Subject: Re: Your messages from this morning
Date: 7 December 2016 at 07:15
To: Claire Lauterbach <claire@privacyinternational.org>
Cc: Aghiath Chbib [AGT] <agchbib@agt-technology.com>

Dear Mr. Lauterbach,

thanks for your mail, I would to help you as much as I can to provide accurate statements.

I would like to assure you that AGT does not own any surveillance technology, and we have been exiting the business of Lawful interception services, few years back, however we have been following all the export regulations related UN, and EU, having said that the technology suppliers are responsible for the export license approval if its needed, and so far we have been never entered to any selling of technologies, where the export licenses has been not approved, if one were needed, please note till few years back majority of surveillance technologies solutions, a export licenses were not required, I m sure u are aware about it.

C ? 8 4 F 8 R A 7 @ L 6 B @ @ 8 A G F G B G ; 8 < A D H < E < 8 F L B H F 8 A 7

1- we have been requested to offer, but we did not sell the RCS surveillance technology for that project.

2-this not accurate as we did not have such technology that time

3-yes we had offered but we did not sell at the end to them

4-internal issue of AGT (private) : Mr. Frans has pass away few years back, its accurate and has nothing to do with any project or export of any technologies.

5-its internal network forensic tool: has with public surveillance tool nothing to do, this for sure

< G @ < ; G ; 4 C C 8 A F 5 H G G ; 8 E 8 J < ? ? 5 8 A B F 8 ? ? F G B 4 A L 4 6 6 B H A G J < G ; B H G : 8 G G < quote, or sales process, adding to that, if we would do it, its the vendor responsibility to obtain the export license, and not the seller, and at the end its south African company, MTN is telecom operator with many location and licenses, if they wanted to use network forensic tool to identify any malware in the network, than its internal issue, this tool is not been made be installed on public networks.

6-this not accurate, it might be RFI or RFQ but never sold.

7-never sold, and if its offered the HW, it is local supply issue, and we can not, will not involve in any importing of HW like dell or others, to any country, not only Syria, beside it was available in SYRIA without any involvement of AGT, as we are not hardware vendor nor distributor.

8- AGT has large portfolio of services and offering around IT, for that : yes we are involved in more than 34 countries, from Data center, Digital forensic to Cyber security defenses tools and related IT services, we have been out of the Lawful interception business for few L 8 4 E F 5 4 6 > 4 A 7 9 B 6 H F < A : B A 6 L 5 8 E 6 E < @ 8 < A I 8 F G < : 4 G < B A 4 A 7 R : ; G < A : 6 E < @ 8 F F G E 4 9 R 6 > < A : 6 4 E G 8 ? F 8 G 6

9. AGT has never met the gentleman, and there is no business what so ever with Sudan(north of south) since the company was established till this moment.

10- we worked with Vastech, and again there was no breach of any international law on that.

11- this is privat issue related to some investment in the UAE in a very far sector from technology.

14- this bite private issue, and could harm the persons related -only by name - to our family, by providing such statements, they could be put in very unpleasant and dangerous positions, just because of your reports, please send me the names u have to comments on them one by one, as is very general statement, and there is few Chbib working in AGT since 2002, as e.g. in EGP, and in Dubai.

C ? 8 4 F 8 ? 8 G @ 8 > A B J < 9 L B H A 8 8 7 4 A L 6 ? 4 E < R 6 4 G < B A B E ; 8 ? C

looking forward to hear from you, by the way some journalist from USA has wrote to us about your report ? it public already ?
rgds
Anas

On Dec 5, 2016, at 15:16, Claire Lauterbach <claire@privacyinternational.org> wrote:

Dear Mr. Chbib,

Annex 6 continued

Response from AGT, December 2016.

On Dec 5, 2016, at 15:16, Claire Lauterbach <claire@privacyinternational.org> wrote:

Dear Mr. Chbib,

Thank you for your messages of this morning.

I request that you raise these issues in writing (by email) so as to maintain an accurate record of your company's views. I regret that we will be unable to discuss these matters orally.

Privacy International is a UK-registered charity. We engage in research, advocacy and litigation on issues in the public interest. The provision of surveillance technologies to governments publicly engaged in repression is one such public interest issue on which we are active.

Our research methods conform to accepted journalistic and public interest research standards. As such we invite you to correct, clarify, or otherwise respond to the key statements we will make.

We would be grateful for your written response to the issues raised in our December 1 letter by the deadline indicated in the letter.

Yours sincerely,

Claire Lauterbach
Researcher
Privacy International
+44(0)2034224321

Mit freundlichen Grüßen / With best regards
Anas Chbib
CEO and Group founder

Advanced German Technology GmbH /