NSA ANT Mobilfunk, 30C3, Jacob Appelbaum, 30 December 2013

Zum Überwachen und Verfolgen von Handys hat die NSA-Abteilung ANT gleich eine ganze Palette von Geräten im Angebot. Das reicht von speziell ausgerüsteten Spezialhandys, mit denen sich ein anderes Han räumlich verfolgen lässt, bis hin zu voll ausgestatteten GSM-Basisstationen, die sich als offizielle Handy-Funkantennen des Netzbetreibers ausgeben können und es dann erlauben, Gespräche oder SMS von Mobiltelefonen in ihrer Reichweite zu überwachen und mitzuschneiden. Man denke nur an die mutmaßliche Überwachung des Handys von Bundeskanzlerin Angela Merkel. Mehrere der spezialisierten Mobilfunk-Basistationen sind auch in der Lage, den genauen Aufenthaltsort eines Handynutzers in ihrer Reichweite zu ermitteln. Ein Gerät namens CANDYGRAM nennen die ANT-Techniker "Telefon-Stolperdraht": Es schickt e SMS in die Kommandozentrale, sobald die Benutzer bestimmter Mobiltelefone in Reichweite sind.

CROSSBEAM ist ein Implantat, das dieselbe Form hat wie ein GSM-Modul, wie es etwa in Notebooks verwendet wird. Es ermöglicht externen Zugriff auf die übertragenen Daten und das System.

CANDYGRAM ist ein GSM-Basisstations-Simulator (für die Frequenzbereiche 900/1800/1900 Mhz), der die Standortdaten der Handys von Zielpersonen über das Senden von nicht angezeigten SMS überprüft.

CYCLONE HX9 ist ein GSM-Funkzellensimulator für Angriffe auf GSM-900-Mobilfunkgeräte. Solche Basisstationen werden benutzt, um Handys abzuhören und Daten von ihnen abzufangen. Es besteht der Verdacht, dass die NSA etwa das Mobiltelefon von Bundeskanzlerin Angela Merkel abgehört hat.

EBSR ist ein aktiver GSM-Zellensimulator, der Angriffe auf GSM-Mobiltelefone in den Frequenzbereichen 900/1800/1900 Mhz ermöglicht.

ENTOURAGE ist ein Funkempfänger zum Orten von GSM- und 3G-Mobiltelefonen, der die GPS-Koordinate der Mobiltelefone von Zielen ermittelt.

Bei GENESIS handelt sich um ein modifiziertes Mobiltelefon für GSM und 3G, mit dem sich Netzparameter und Frequenznutzungen feststellen sowie Mobiltelefone orten lassen.

NEBULA ist ein GSM-Zellensimulator für 2G-Netze (900 Mhz) und 3G-Netze (2100 Mhz).

TYPHON HX: Ein GSM-Zellensimulator für alle weltweit gängigen GSM-Frequenzen (850/900/1800/1900 Mhz). Damit lassen sich Mobiltelefone abhören.

WATERWITCH ist ein Gerät, mit dem sich der exakte Standort der Mobiltelefone von Zielpersonen in unmittelbarer Nähe feststellen lässt.

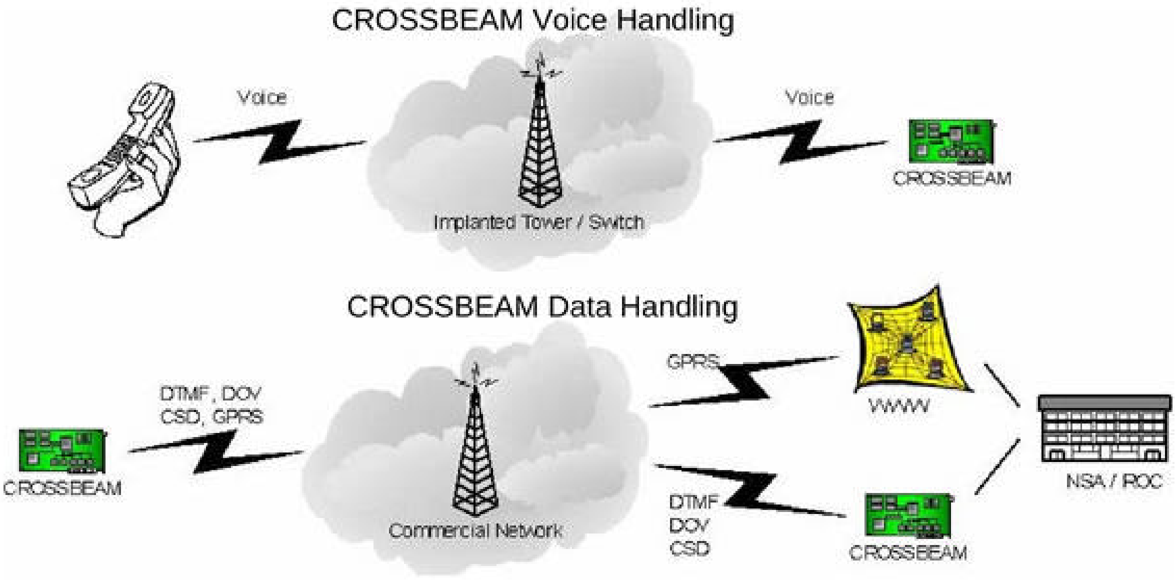
CROSSBEAM

ANT Product Data

(TS//SI//REL) CROSSBEAM is a GSM module that mates a modified commercial cellular product with a WAGONBED controller board.

08/05/08

(TS//SI//REL) CROSSBEAM is a reusable CHIMNEYPOOL-compliant GSM communications module capable of collecting and compressing voice data. CROSSBEAM can receive GSM voice, record voice data, and transmit the received information via connected modules or 4 different GSM data modes (GPRS, Circuit Switched Data, Data Over Voice, and DTMF) back to a secure facility. The CROSSBEAM module consists of a standard ANT architecture embedded computer, a specialized phone component, a customized software controller suite and an optional DSP (ROCKYKNOB) if using Data Over Voice to transmit data.



Status: Limited Supply Available
Delivery: 90 days for most configurations

Unit Cost: $4k

POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov
ALT POC: [redacted], S3223, [redacted], [redacted]@nsa.ic.gov

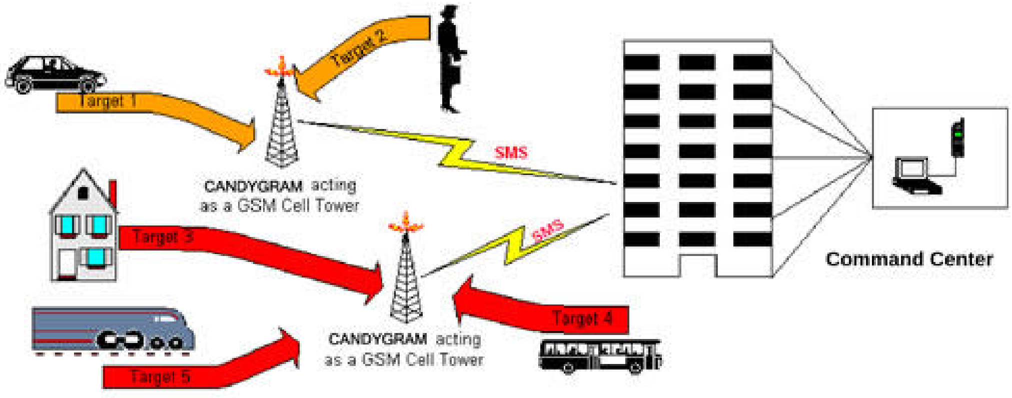
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

CANDYGRAM

GSM Telephone Tripwire

(S//SI//REL) Mimics GSM cell tower of a target network. Capable of operations at 900, 1800, or 1900 MHz. Whenever a target handset enters the CANDYGRAM base station's area of influence, the system sends out an SMS through the external network to registered watch phones.

06/20/08


Target 2
Target 1
SMS
CANDYGRAM acting as a GSM Cell Tower
Target 3
SMS
Command Center
Target 4
CANDYGRAM acting as a GSM Cell Tower
Target 5

(S//SI//REL) CANDYGRAM Operational Concept

(S//SI//REL) Typical use scenarios are asset validation, target tracking and identification as well as identifying hostile surveillance units with GSM handsets. Functionality is predicated on apriori target information.

(S//SI//REL) System HW

- GPS processing unit
- Tri-band BTS radio
- Windows XP laptop and cell phone*
- 9" wide x 12 " long x 2 " deep
- External power (9-30 VDC).

*Remote control software can be used with any connected to the laptop (used for communicating with the CANDYGRAM unit through text messages (SMS).

(S//SI//REL) SW Features

- Configurable 200 phone number target deck.
- Network auto-configuration
- Area Survey Capability
- Remote Operation Capability
- Configurable Network emulation
- Configurable RF power level
- Mutli-Units under single C&C
- Remote restart
- Remote erasure (not field recoverable)

Status: Available 8 mos ARO

Unit Cost: approx $40K

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

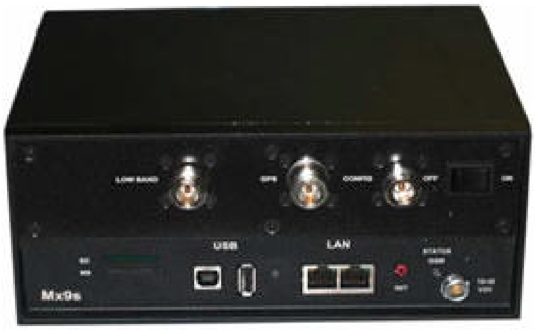
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

CYCLONE Hx9

Base Station Router

(S//SI//FVEY) EGSM (900MGz) macro-class Network-In-a-Box (NIB) system. Uses the existing Typhon GUI and supports the full Typhon feature base and applications.

(S//SI//REL) Operational Restrictions exist for equipment deployment.



➢ **(S//SI//REL) Features:**

- EGSM 900MHz
- Macro-class (+43dBm)
- 32+Km Range
- Optional Battery Kits
- Highly Mobile and Deployable
- Integrated GPS, MS, & 802.11
- Voice & High-speed Data
- GSM Security & Encryption

➢ **(S//SI//REL) Advanced Features:**

- GPS – Supporting Typhon applications
- GSM Handset Module – Supports auto-configuration and remote command and control features.
- 802.11 – Supports high speed wireless LAN remote command and control

➢ **(S//SI//REL) Enclosure:**

- 3.5"H x 8.5"W x 9"D
- Approximately 8 lbs
- Actively cooled for extreme environments

➢ **(S//SI//REL) Cyclone Hx9 System Kit:**

- Cyclone Hx9 System
- AC/DC power converter
- Antenna to support MS, GPS, WIFI, & RF
- LAN, RF, & USB cables
- Pelican Case
- (Field Kit only) Control Laptop and Accessories

➢ **(S//SI//REL) Separately Priced Options:**

- 800 WH LiIon Battery Kit

➢ **(S//SI//REL) Base Station Router Platform:**

- Overlay GSM cellular communications supporting up to 32 Cyclone Mx9 systems providing full mobility and utilizing a VoIP back-haul.
- GPRS data service and associated application

Unit Cost: $70K for two months

Status: Just out of development, first production runs ongoing.

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

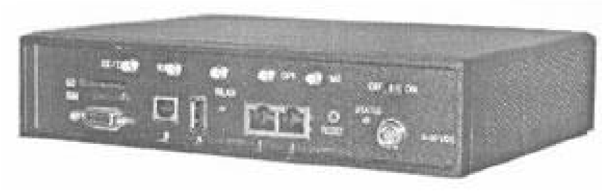
EBSR

Low Power GSM Active Interrogator

(S//SI//REL) Multi-purpose, Pico class, tri-band active GSM base station with internal 802.11/GPS/handset capability.

01/27/09

(S//SI//REL) Operational Restrictions exist for equipment deployment.



➢ (S//SI//REL) Features:

- LxT Model: 900/1800/1900MHz
- LxU Model: 850/1800/1900MHz
- Pico-class (1Watt) Base station
- Optional Battery Kits
- Highly Mobile and Deployable
- Integrated GPS, MS, & 802.11
- Voice & High-speed Data
- SMS Capability

➢ (S//SI//REL) Enclosure:

- 1.9"H x 8.6"W x 6.3"D
- Approximately 3 lbs
- Actively cooled for extreme environments

➢ (S//SI//REL) EBSR System Kit:

- EBSR System
- AC/DC power converter
- Antennas to support MS, GPS, WIFI, & RF
- LAN, RF, & USB cables
- Pelican Case
- (Field Kit only) Control Laptop and Accessories

➢(S//SI//REL) Separately Priced Options:

- 90 WH LiIon Battery Kit

➢ (S//SI//REL) Base Station Router Platform:

- Multiple BSR units can be interconnected to form a macro network using 802.3 and 802.11 back-haul.
- Supports Landshark/Candygram capabilities.

Status:

Unit Cost: $40K

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

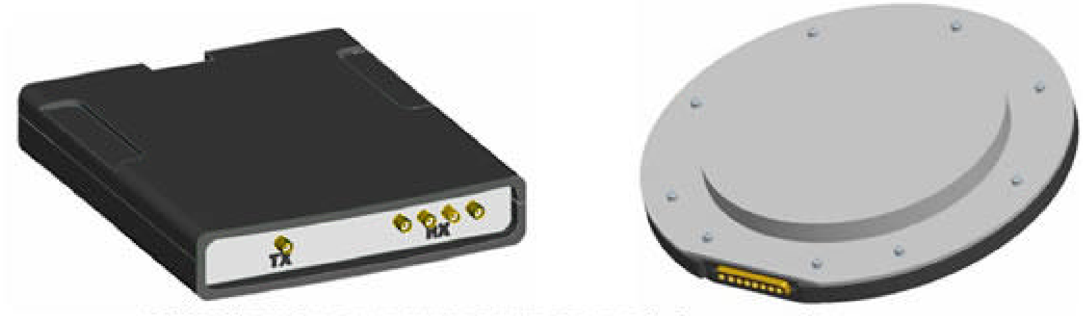
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

ENTOURAGE

(S//SI//REL) Direction Finding on HollowPoint Platform

(S//SI//REL) Direction Finding application operating on the HOLLOWPOINT platform. The system is capable of providing line of bearing for GSM/UMTS/ CDMA2000/FRS signals. A band-specific antenna and laptop controller is needed to compliment the HOLLOWPOINT system and completes the ground based system.

01/27/09



(S//SI//REL) HOLLOWPOINT SDR Platform and Antenna

(S//SI) The ENTOURAGE application leverages the 4 Software Defined Radio (SDR) units in the HOLLOWPOINT platform. This capability provides an "Artemis-like" capability for waveforms of interest (2G,3G,others). The ENTOURAGE application works in conjunction with the NEBULA active interrogator as part of the Find/Fix/Finish capabilities of the GALAXY program.

➢ **(S//SI//REL) Features:**

- Software Defined Radio System
- Operating range 10MHz – 4GHz
- 4 Receive paths, all synchronized
- 1 Transmit path
- DF capability on GSM/UMTS/CDMA2000/ FRS signals
- Gigabit Ethernet
- Integrated GPS
- Highly Mobile and Deployable

➢ **(S//SI//REL) Enclosure:**

- 1.8"H x 8.0"W x 8.0"D
- Approximately 3 lbs
- 15 Watts
- Passively cooled

➢ **(S//SI//REL) Future Developments:**

- WiMAX
- WiFi
- LTE

Status: The system is in the final testing stage and will be in production Spring 09.

Unit Cost: $70K

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

GENESIS

Covert SIGINT Transceiver

(S//SI//REL) Commercial GSM handset that has been modified to include a Software Defined Radio (SDR) and additional system memory. The internal SDR allows a witting user to covertly perform network surveys, record RF spectrum, or perform handset location in hostile environments.

01/27/09

(S//SI//REL) GENESIS Handset

(S//SI//REL) The GENESIS systems are designed to support covert operations in hostile environments. A witting user would be able to survey the local environment with the spectrum analyzer tool, select spectrum of interest to record, and download the spectrum information via the integrated Ethernet to a laptop controller. The GENESIS system could also be used, in conjunction with an active interrogator, as the finishing tool when performing Find/Fix/Finish operations in unconventional environments.

➢ **(S//SI//REL) Features:**

- Concealed SDR with Handset Menu Interface
- Spectrum Analyzer Capability
- Find/Fix/Finish Capability
- Integrated Ethernet
- External Antenna Port
- Internal 16 GB of storage
- Multiple Integrated Antennas

➢ **(S//SI//REL) Future Enhancements:**

- 3G Handset Host Platform
- Additional Host Platforms
- Increased Memory Capacity
- Additional Find/Fix/Finish Capabilities
- Active Interrogation Capabilities

Status: Current GENESIS platform available. Future platforms available when developments are completed.

Unit Cost: $15K

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

NEBULA

Base Station Router

01/27/09

(S//SI//FVEY) Multi-Protocol macro-class Network-In-a-Box (NIB) system. Leverages the existing Typhon GUI and supports GSM, UMTS, CDMA2000 applications. LTE capability currently under development.

(S//SI//REL) Operational Restrictions exist for equipment deployment.

➢ **(S//SI//REL) Features:**

- Dual Carrier System
- EGSM 900MHz
- UMTS 2100MHz
- CDMA2000 1900MHz
- Macro-class Base station
- Optional Battery Kits
- Highly Mobile and Deployable
- Integrated GPS, MS, & 802.11
- Voice & High-speed Data

➢ **(S//SI//REL) Advanced Features:**

- GPS – Supporting NEBULA applications
- Designed to be self-configuring with security and encryption features
- 802.11 – Supports high speed wireless LAN remote command and control

➢ **(S//SI//REL) Enclosure:**

- 8.5"H x 13.0"W x 16.5"D
- Approximately 45 lbs
- Actively cooled for extreme environments

➢ **(S//SI//REL) NEBULA System Kit:**

- NEBULA System
- 3 Interchangeable RF bands
- AC/DC power converter
- Antenna to support MS, GPS, WIFI, & RF
- LAN, RF, & USB cables
- Pelican Case
- (Field Kit only) Control Laptop and Accessories

➢ **(S//SI//REL) Separately Priced Options:**

- 1500 WH LiIon Battery Kit

➢ **(S//SI//REL) Base Station Router Platform:**

- Multiple BSR units can be interconnected to form a macro network using 802.3 and 802.11 back-haul.
- Future GPRS and HSDPA data service and associated applications

Status:

Unit Cost: $250K

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

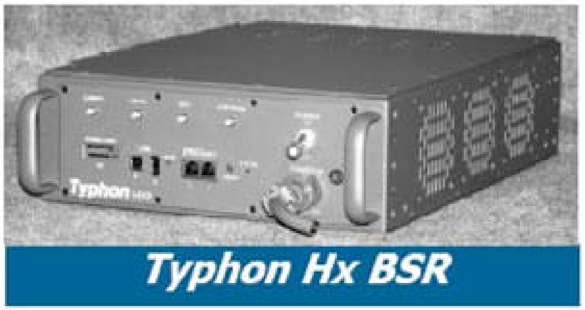
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TYPHON HX

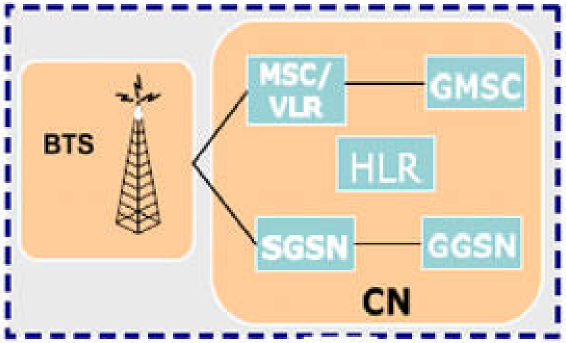
GSM Base Station Router

(S//SI//FVEY) Base Station Router - Network-In-a-Box (NIB) supporting GSM bands 850/900/1800/1900 and associated full GSM signaling and call control.

06/20/08



Typhon Hx BSR

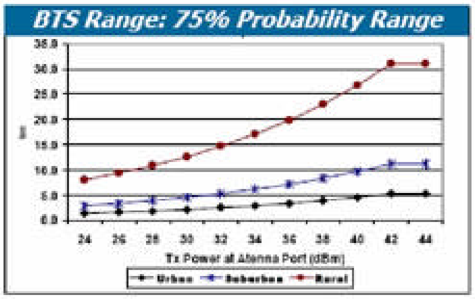


Typhon BSR

(S//SI//FVEY) Tactical SIGINT elements use this equipment to find, fix and finish targeted handset users.

(S//SI) Target GSM handset registers with BSR unit.

(S//SI) Operators are able to geolocate registered handsets, capturing the user.



(S//SI//REL) The macro-class Typhon is a Network-In-a-Box (NIB), which includes all the necessary architecture to support Mobile Station call processing and SMS messaging in a stand-alone chassis with a pre-provisioning capability.

(S//SI//REL) The Typhon system kit includes the amplified Typhon system, OAM&P Laptop, cables, antennas and AC/DC power supply.

(U//FOUO) An ***800 WH LiIon Battery kit is offered separately.***

(U) A bracket and mounting kit are available upon request.

Typhon Hx Priced Options

Deliverable	Duration	FFP COST ea.
1 to 25 units	4 Months	$175,800

Typhon Model/Color	Order Code (& Tool Spare kit)
Hx8/Black (GSM850)	G1004164 & G1004140
Hx8/Green (GSM850)	G1004161 & G1004137
Hx9/Black (EGSM900)	G1003727 & G1002665
Hx9/Green (EGSM900)	G1003726 & G1002037
Hx18/Black (DCS1800)	G1004165 & G1004141
Hx18/Green (DCS1800)	G1004162 & G1004138
Hx19/Black (PCS1900)	G1004166 & G1004142
Hx19/Green (PCS1900)	G1004163 & G1004139

(U) **Status:** Available 4 mos ARO

(S//SI//REL) Operational Restrictions exist for equipment deployment.

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

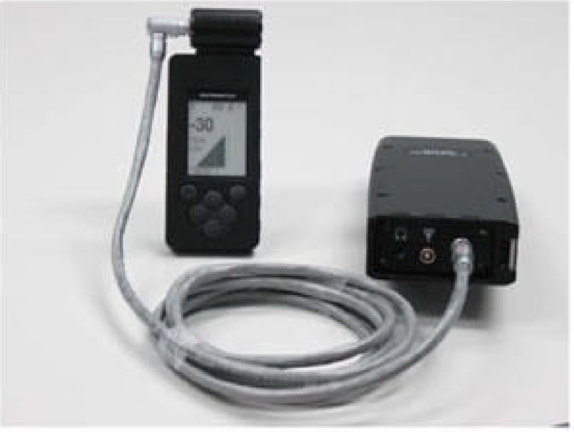
WATERWITCH

Handheld Finishing Tool

(S//SI) Hand held finishing tool used for geolocating targeted handsets in the field.

07/30/08

(S//SI) Features:



(S//SI) WATERWITCH Handset DF Set

- Split display/controller for flexible deployment capability
- External antenna for DFing target; internal antenna for communication with active interrogator
- Multiple technology capability based on SDR Platform; currently UMTS, with GSM and CDMA2000 under development
- Approximate size 3" x 7.5" x 1.25" (radio), 2.5" x 5" x 0.75" (display); radio shrink in planning stages
- Display uses E-Ink technology for low light emissions

(S//SI) Tactical Operators use WATERWITCH to locate handsets (last mile) where handset is connected to Typhon or similar equipment interrogator. WATERWITCH emits tone and gives signal strength of target handset. Directional antenna on unit allows operator to locate specific handset.

Status: Under Development. Available FY-2008 **Unit Cost:**
LRIP Production due August 2008

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108