

INTERAGENCY COOPERATION CONTRACT

VTAUS CH#

22789

THIS CONTRACT AND AGREEMENT is entered into by and between the governmental entities shown below as Contracting parties, pursuant to the authority granted and in compliance with the provisions of the Interagency Cooperation Act, Chapter 771, Texas Government Code.

SECTION I. CONTRACTING PARTIES

Receiving Agency: Department of Information Resources (DIR)
300 W. 15th Street, Suite 1300
Austin, Texas 78701
512/475-4700; 512/475-4759 Fax

Performing Agency: The University of Texas Austin
Information Security Office
1 University Station Stop G9805
Austin, TX 78712

SECTION II. STATEMENT OF SERVICES TO BE PERFORMED

- A. **OVERVIEW.** The Information Security Office of The University of Texas at Austin (UT) will provide a security sensor (Panopticon) and monitoring and alerting for all confirmed malicious or suspicious traffic or indicators of compromise to the DIR Network Security Operations Center (NSOC). Schedule A, Statement of Work (SOW) is attached hereto and contains further details and expectations of the services to be performed.
- B. **NOTIFICATION.** The primary contacts designated for any changes in service are as follows:
- a. **Performing Agency:** Cam Beasley
Email: cam@utexas.edu
Phone: (512) 475-9476
 - b. **Receiving Agency:** Jeremy Wilson
Email: Jeremy.wilson@dir.texas.gov
Phone: (512) 475-0602

SECTION III. FEES FOR SERVICES AND CONTRACT AMOUNT

This Panopticon monitoring and alerting service is being provided to the DIR Network Security Operations Center (NSOC) at a rate of \$150,000.00 annually or \$12,500.00 per month. The effective date of this contract will be the date the contracting parties dually execute this agreement.

SECTION IV. PAYMENT FOR SERVICES

The Receiving Agency will pay for Services received from the performing agency upon contract being executed and signed by both parties. Receiving Agency will pay the monthly recurring fee per the attached SOW Schedule A.

SECTION V. TERM OF CONTRACT

This Contract is effective from date of last signature through August 31, 2016 unless terminated earlier by written agreement of the parties. At the end of the contract the parties may renew the services upon mutual agreement on an annual basis until terminated by either party.

SECTION VI. GENERAL PROVISIONS

- A. **PUBLIC RECORDS.** It shall be the independent responsibility of The University of Texas and DIR to comply with the provisions of Chapter 552, Texas Government Code (the Public Information Act), as they apply to their respective information. Neither party is authorized to receive public information requests or take any other action under the Public Information Act on behalf of the other party.
- B. **BINDING EFFECT.** The parties hereto bind themselves to the faithful performance of their respective obligations under this contract.
- C. **AMENDMENTS.** This contract shall not become valid until signed by duly authorized representatives of both parties, and may not be amended except by written document signed by both parties hereto.
- D. **Confidentiality Obligation.** UT acknowledges that information regarding the infrastructure and security of DIR information systems, that relate to specifically and uniquely to the vulnerability of DIR information systems or otherwise marked as confidential by DIR must be protected. Both parties agree to hold any confidential information received during the timeframe that the contract is in effect and thereafter in confidence to the same extent and the same manner as each party protects its own confidential information. The Parties agree to use all reasonable steps to ensure that Confidential Information received under this

agreement is not disclosed in violation of this section. These confidentiality obligations shall survive the completion of this contract.

SECTION VI. CERTIFICATIONS

THE UNDERSIGNED CONTRACTING PARTIES do hereby certify that:

- A. The services specified above are necessary and essential and are properly within the statutory functions and programs of the affected agencies of State Government;
- B. The proposed arrangement serve the interest of efficient and economical administration of State Government; and
- C. The services, supplies or materials contracted for are not required by Section 21 of Article 16 of the Constitution of Texas to be supplied under contract given to the lowest responsible bidder nor is this Contract prohibited by Texas Government Code, Section 771.003, Subsections (b) or (c).

Receiving Agency further certifies that it has the authority to contract for the above services pursuant to the provisions of Chapter 2054, Texas Government Code, and Chapter 71, Texas Education Code.

DIR further certifies that it has the authority to perform the services contracted for pursuant to the authority of Texas Government Code, Chapters 771 and 2054.

THIS PORTION OF THE PAGE INTENTIONALLY LEFT BLANK

PERFORMING AGENCY:

**THE UNIVERSITY OF TEXAS
AUSTIN**

Linda Shaunessy

Printed Name: Linda Shaunessy
UT Business Contracts

Date: 8/17/2015

RECEIVING AGENCY:

**TEXAS DEPARTMENT OF
INFORMATION RESOURCES**

*Stan Lyle FOR
WAYNE EGELER*

Printed Name: Wayne Egeler Director CTS

Date: 8/25/15

Legal: Abbott 8-24-15

**Department of Information Resources
Statement of Work (SOW)**

UT

Schedule A to DIR-CTS-IAC-003

***Panopticon Intrusion Detection
System (IDS) Service***

***DIR Network Security Operations
Center (NSOC)***

8/15/2015

Department of Information Resources Statement of Work (SOW)

1. Introduction

Panopticon is a network monitoring tool developed by the University of Texas (UT) to assist their Chief Information Security Officer in monitoring and defending their own networks. UT is similar to the Texas Department of Information Resources (DIR) in that it has a large scale network with many diverse users and a small staff to manage all alerts and incidents on its network. Panopticon helps a small group of analysts determine the most critical events that are happening in real time. One particular feature of Panopticon is its Sensitive Number Finder (SENF) algorithm. This filter can be set to look for credit cards, social security numbers, driver's license numbers and many other sensitive numbers that are being transmitted in clear text (unencrypted) over the internet. It can be configured to alert on batches of 2, or 10 or any number that is necessary for DIR to investigate whether an unauthorized transaction might have taken place. Normally when batches of these numbers are being transmitted in clear text and not encrypted there is an indicator of either unsecure programming or architecture or an actual data compromise is ongoing. Since this device is passive and does no blocking it is a good solution for our environment. Panopticon also has a number of other custom signatures and filters that UT develops in house that help identify compromised hosts on our network.

2. Background

UT is one of the premier institutions of higher education in the State of Texas and is also a State agency. The fact that DIR can utilize UT's own Panopticon device and that it comes with monitoring from UT's CISO and analysts is a great value to both organizations. It makes sense for both organizations to share intelligence and strategy as they have a customer in common the Texas Education Agency (TEA). TEA utilizes UT's network but is also a DIR Data Center customer. If they were under attack it would be helpful to have all interested parties react and be aware of any malicious activity. In addition UT and DIR have partnered in some other relevant areas for security. UT is utilizing DIR for collocation server space for a secure application that they have in case there is a true Disaster Recovery (DR) scenario that affects their network. There are also some data visualization projects and aspects of UT's Splunk implementation that DIR is looking to leverage UT's knowledge on. These are of course independent of this purchase but demonstrate the value in sharing intelligence across the two organizations.

3. Scope

The scope for this SOW applies to just the Panopticon monitoring and alerting service. UT will analyze all alerts out of Panopticon for accuracy and then forward any alerts to the DIR NSOC for action. The DIR NSOC will analyze any alerts received from UT for validity and will take action as necessary to confirm these alerts. Both parties will work together to modify or enhance the service to continue to provide the best monitoring and alerting for the DIR environment.

4. Deliverables

- UT will deliver monthly Panopticon Alert Summary Report to DIR on/by the 5th of each month for the preceding months activity.
- UT will ensure updated filters and signatures are applied to the Panopticon platform
- UT will provide DIR with Packet Captures (PCAPs) for alerts when requested by DIR
- Both parties will ensure a secure VPN tunnel is maintained between UT Austin and DIR for access to device

**Department of Information Resources
Statement of Work (SOW)**

5. Reports and Meetings

DIR and UT Austin will meet on an as-needed basis. No pre-scheduled meetings arranged at this time. Monthly report noted in Deliverables section.

6. Service Level Agreement

- UT Austin will continue to provide alerting from Panopticon platform to DIR for the following types of alerts. In addition to the monthly report, DIR shall receive follow up alerts for any recurring activity at timeframe not to exceed every 30 minutes until questionable activity is no longer detected. This means for any compromised host when Panopticon detects recurring activity DIR will be notified every 30 minutes until the activity or traffic stops. This will allow DIR to confirm if any recurring activity is taking place. Compromised host notifications from Panopticon will be generated in near real-time of the actual event and automatically distributed to DIR. Sensitive number finder results from Panopticon will be verified by UT Austin in a timely manner to ensure accuracy and will be distributed to DIR as quickly as reasonably possible. Panopticon can be set to alert for different thresholds and DIR and UT will mutually agree upon those criteria if they need to be adjusted. Upon written request from DIR UT will adjust the alerting threshold no later than 5 business days from receiving request.
- In the event of a system failure, UT Austin will make reasonable efforts to work with DIR to replace Panopticon system within one week. If due to no fault of DIR (ex for faults of DIR would be DIR fails to provide adequate power, connectivity or feed traffic etc.) the system stays down for more than one week DIR will receive a credit for each day after the 7 day period from initial notification to UT that Panopticon is down of 410.96 per day until the Panopticon system is recovered and fully functional.
- Current platform will remain in place until DIR gateway Internet speeds exceed 10Gbps and DIR will notify UT Austin prior to the 10Gbps threshold being exceeded within an adequate amount of time to effectively manage the upgrade.
- UT Austin will continue to provide the most up-to-date custom signatures and filters for Panopticon in order for DIR to receive the most accurate and timely alerting of compromised hosts and sensitive numbers from UT Austin.
- UT Austin and DIR will continue to collaborate on the secure VPN tunnel between the DIR NSOC and UT Austin security operations center in order to ensure UT has access to the Panopticon sensor at DIR NSOC for alerting purposes.

7. Period of Performance

Performance will begin upon dually executed signature of this SOW and will remain in place through August 31, 2016. Services may be renewed on an annual basis upon mutual agreement and update of SOW by both parties for up to 3 additional one year renewals.

8. Invoices

Payment for services will be made monthly based on services rendered at the amount stated in this SOW and based on the PO in place for these services. Any changes to the services or failed SLAs that may impact pricing will be accounted for and, where necessary, mutually agreed to by both parties and noted in the PO through a Purchase Order Change Notice (POCN).

**Department of Information Resources
Statement of Work (SOW)**

9. Customer/Vendor-Furnished Equipment and Work Space

UT Austin provide the Cisco Sourcefire Panopticon chassis at the DIR NSOC. DIR NSOC will continue to provide adequate rack space, power, and cooling for the appliance. DIR will provide access to designated UT personnel as needed. UT personnel will be escorted while on-site in the NSOC facility.

10. Vendor Responsibilities

UT Austin will:

- Provide monitoring and alerting in conjunction with this SOW
- Provide ongoing service and maintenance of Panopticon appliance
- Provide monthly summary reports
- Continue to provide DIR with Packet Captures (PCAPs) for alerts when requested by DIR
- Continue to collaborate with DIR on secure connectivity between security operations center
- Ensure secure VPN tunnel is maintained between UT Austin and DIR

11. Customer Responsibilities

DIR will:

- Provide adequate rack space, power and climate control for equipment housed at DIR NSOC
- Ensure secure VPN tunnel is maintained between UT Austin and DIR
- Provide site access as needed to Panopticon equipment
- Provide network diagram and IP mapping schema in order to facilitate best possible alerting from UT to DIR
- Continue to provide UT Austin with feedback on alerts received from Panopticon based on DIR NSOC analysis

12. Pricing

Services rendered will be at the price listed below for each month the SOW is effective.

Pricing Sheet

| Item | Deliverable Name | Price |
|------|--------------------------|----------|
| 1 | Monthly Recurring Charge | \$12,500 |
| | | |
| | | |

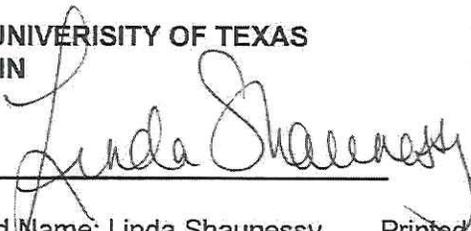
REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK

Department of Information Resources
Statement of Work (SOW)

BY SIGNING BELOW, THE UNDERSIGNED AGREE THEY ARE BOUND BY THE TERMS OF THIS SOW AND THE AGREEMENT.

PERFORMING AGENCY:

THE UNIVERSITY OF TEXAS
AUSTIN



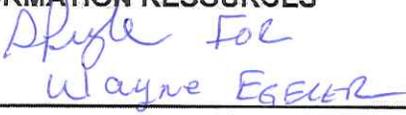
Printed Name: Linda Shaunessy
UT Business Contracts

Date:

8/17/2015

RECEIVING AGENCY:

TEXAS DEPARTMENT OF
INFORMATION RESOURCES



Printed Name: Wayne Egeler, Director CTS

Date:

8/26/15

Legal:

CPH-MW-8-24-15