DIVISION OF INFORMATION SYSTEMS & TELECOMMUNICATIONS (DIST)

Request for Proposal, RFP/2018/1077

Annex A

Terms of Reference for UNHCR ICT Cybersecurity Incident Managed Detection and Response Services Agreement

United Nations
High Commissioner for Refugees

Table of Contents

TABLE OF CONTENTS **2**
1 INTRODUCTION **4**
1.1 INTRODUCTION TO UNHCR 4
1.2 PROPOSAL BACKGROUND 4
1.3 OBJECTIVES 4
1.3.1 Organizational Context *4*
1.3.2 Operational Context *4*
1.3.3 Business Objectives *5*
1.3.4 RFP Objectives *5*
2 CURRENT UNHCR ICT ENVIRONMENT **6**
2.1 UNHCR LANDSCAPE 6
2.2 DIST ORGANIZATION 7
2.3 ICT CYBERSECURITY AT UNHCR 8
2.3.1 Current Status *8*
2.3.2 Challenges *9*
3 ICT CYBERSECURITY MDR SERVICE REQUIREMENTS **10**
3.1 SERVICES TO BE PROVIDED 10
3.1.1 Service Description *10*
3.1.2 Service Scope and volumes *11*
4 INSTRUCTIONS FOR BIDDERS – TECHNICAL PROPOSAL **12**
4.1 COMPANY ASSESSMENT 12
4.1.1 Company Profile and Background *12*
4.1.2 Financial Stability *12*
4.1.3 Relevant Experience *12*
1. ICT Cybersecurity Incident Managed Detection and Response Experience 12
2. Relevant Environment Experience 12
4.1.4 Compliance Requirements *13*
4.1.5 Customer References *13*
4.1.6 Global Reach *14*
1. Locations/Resources 14
2. Work Permits 14
4.1.7 Relationship Management *14*
4.1.8 Security Procedures *14*
4.1.9 Uniqueness *14*
4.1.10 Additional Proposal Sections (optional) *15*
5 INSTRUCTIONS FOR BIDDERS – COMMERCIAL PROPOSAL **16**
5.1 MANNER OF SUBMISSION 16
5.2 SALES ENGAGEMENT PROCESS 16
5.2.1 Contractual Terms *16*
5.2.2 Fee Structure and Price *16*
6 ADDITIONAL INFORMATION **17**
6.1 EVALUATION OF PROPOSALS 17
6.2 TERM OF CONTRACT 17
6.3 UNHCR GENERAL CONDITIONS FOR THE PROVISION OF SERVICES 17
6.4 UNHCR SPECIAL CONDITIONS FOR CLOUD COMPUTING 17
6.5 UNHCR SPECIAL DATA PROTECTION CONDITIONS 17
6.6 UNHCR VENDOR REGISTRATION FORM 17
6.7 UN SUPPLIER CODE OF CONDUCT 18

6.8 PERFORMANCE 18
6.9 SECURITY PROCEDURES 18
6.9.1 Business Recovery. *19*
6.10 INVOICES 19
6.11 PAYMENT TERMS/PRICE POLICY 19
6.11.1 Payment Terms *19*
6.11.2 Service Level linked Payments *20*
6.12 TRAVEL AND MISSIONS 20
6.13 INSTRUCTIONS ON COMPLETING THE SPREADSHEETS 20

1 Introduction

1.1 Introduction to UNHCR

The U.N. General Assembly established the Office of the United Nations High Commissioner for Refugees (UNHCR) in 1950 to provide protection and assistance to refugees. Today, UNHCR is one of the world's principal humanitarian agencies. It has more than 10,000 staff helping 60 million people in 130 countries. For more information, please see http://www.unhcr.org/.

1.2 Proposal Background

The purpose of this Request for Proposal (RFP) is to establish a Contract with a Service Provider to deliver Cybersecurity Incident Managed Detection and Response (MDR) services in support of UNHCR's planned Information Communications and Technology (ICT) Cybersecurity Transformation Program.

The initial period of this Contract will be for three (3) years, extendable for up to five (5) additional one (1) year periods (i.e., 3+1+1). This RFP invites potential bidders to submit a proposal for ICT Cybersecurity Incident Managed Detection and Response Services which will meet UNHCR's initial objectives.

It is strongly recommended that this document be read thoroughly.. Failure to observe the procedures laid out in this document and the covering letter may result in disqualification from the evaluation process.

1.3 Objectives

1.3.1 Organizational Context

The Division of Information Systems and Telecommunications (DIST) provides Information and Communication Technology (ICT) services, playing a vital role in supporting UNHCR's mission.

DIST is responsible for the maintenance, evolution and support of UNHCR's ICT systems, including developing the organization's strategic ICT direction and supporting the related ICT project initiatives. DIST provides ICT services and support to meet the needs of all Divisions, Bureaux and Field Offices within the organization while ensuring that necessary governance mechanisms are in place and standards are adopted and adhered to.

The Service Provider so engaged will provide the ICT Cybersecurity MDR as a service to UNHCR globally, and when required, will provide dedicated remote and on-site resources to UNHCR's locations primarily in Geneva, Switzerland and Amman, Jordan, with oversight provided by UNHCR's DIST Deputy Director, ICT Operations (see Section 2.2 for more information on the DIST organization).

1.3.2 Operational Context

UNHCR's primary purpose is to safeguard the rights and well-being of refugees (also known as Persons of Concern, or PoC). Even if UN Organizations like UNHCR have non-profit

purposes, they are vulnerable due to the sensitive data they possess. For UNHCR, PoC data is the most valuable information that exists and it must be adequately protected. UNHCR wants to ensure strong security at the right cost for their most valuable information, systems and processes, with a specific focus on PoC data.

A recent cybersecurity assessment commissioned by UNHCR identified potential threat actors with different motivations which could be interested in UNHCR's PoC data, and a number of potential risk areas. Some of the shortcomings identified in the assessment included:

- Security Governance requires improvement and lacks consistency throughout UNHCR; and not all required security policies and guidance have been formalized yet;
- Limited detection capabilities exist around security event monitoring, cyber analytics, cyber threat intelligence and limited penetration testing & vulnerability scanning;
- Inconsistent cybersecurity procedures/approaches are not in place, nor is there a consistent focus on understanding and remediating the root cause of the underlying vulnerabilities.

. There is a clear need to improve the maturity and overall security posture of UNHCR's ICT assets.

1.3.3 Business Objectives

As a result of this assessment, UNHCR has initiated an ICT Cybersecurity Transformation program to put in place strong and consistent ICT security controls.

In order to mitigate the main security gaps and risks that were identified, , UNHCR is expecting to execute a set of 10-12 ICT Cybersecurity projects over the next 3-5 years, beginning with 2018, in areas such as Identity & Access Management, Infrastructure Security, Data Loss Prevention and Security Event Monitoring.

The overall objective is to enhance the security of its "crown jewels", in particular that of PoC data (and other critical data) and to achieve a desired maturity level for organizational ICT Cybersecurity.

The implementation of the MDR services in scope of this RFP has been identified as one of the priority components of the strategy.

1.3.4 RFP Objectives

This Request for Proposal is intended to give potential Service Providers the necessary information to enable them to submit proposals in the required format and timescale that best meet UNHCR's objectives. In addition, it describes how such proposals will be evaluated and sets out the way in which any necessary communications between potential providers and UNHCR should be handled. UNHCR is not seeking a compilation of standard materials and marketing collateral; relevance and quality, rather than quantity, should be considered while proposals are being assembled.

2 Current UNHCR ICT Environment

2.1 UNHCR Landscape

UNHCR staff work in 130 countries around the world, from major capitals to remote and often dangerous locations. About 7% of staff are based at the Geneva, Switzerland headquarters. Along with the Global Service Centers in Budapest, Copenhagen and Amman, these people provide support for the rest of UNHCR, including key administrative functions. Around 87% of staff are based in "field" locations. The span of UNHCR locations is shown in Figure 1.

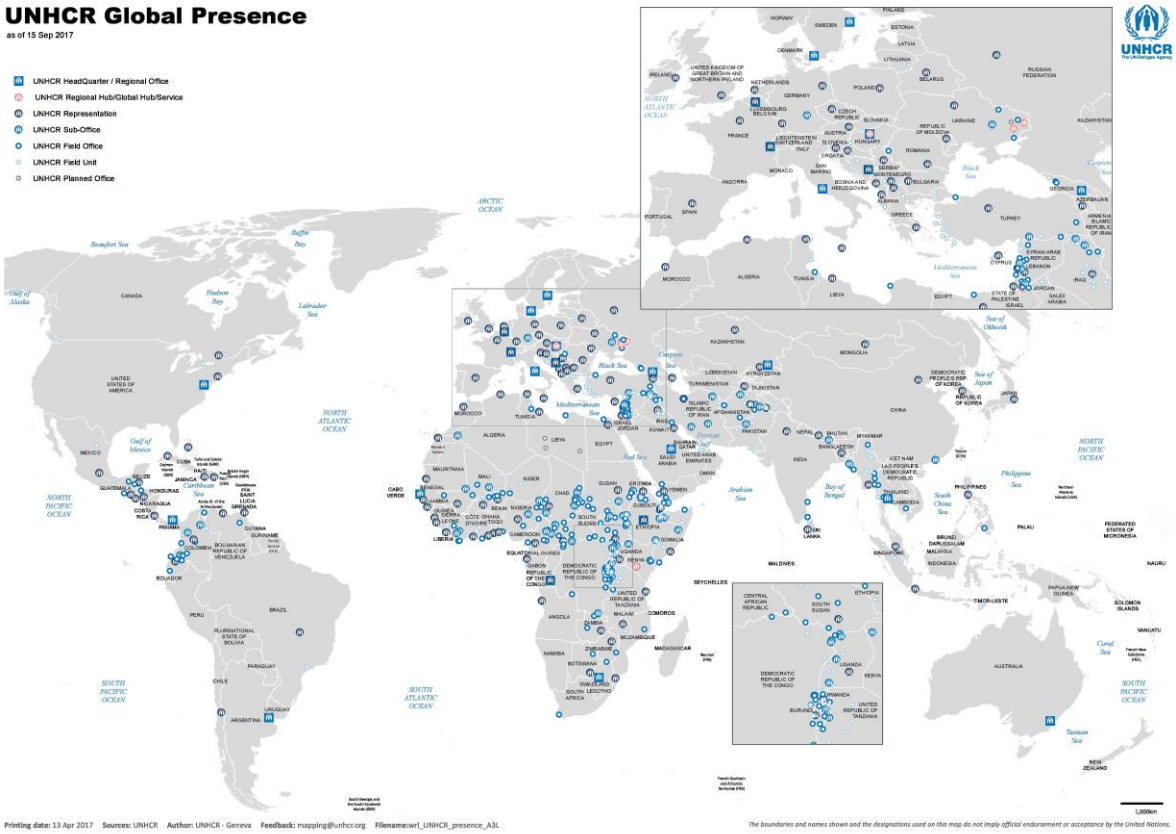

Figure 1 – UNHCR Worldwide Locations

UNHCR's ICT Assets in scope are distributed globally across over 130 countries, and can be summarized as follows:

- 16,000 users, with the large majority located in field operations
- 16,000 Microsoft Windows Workstations, and additional mobile and personal devices used by UNHCR users
- 30,000 networked devices, across LANs in over 550+ field sites
- 750 central servers, distributed between corporate data centers and cloud service providers
- 2,000 field servers distributed across 350+ field sites, of which 600+ containing confidential data
- 6 critical and 40 less critical corporate applications
- 10+ regional or local critical applications
- 15Gbps of dedicated Internet bandwidth, distributed across all sites

- 300Mbps of dedicated VSAT bandwidth for deep field locations

2.2 DIST Organization

The Division of Information Systems and Telecommunications (DIST) provides Information and Communication Technology (ICT) services, playing a vital role in supporting UNHCR's mission. DIST is responsible for the maintenance, evolution and support of UNHCR's ICT systems, including developing the organization's strategic ICT direction and supporting the related ICT project initiatives. DIST provides ICT services and support to meet the needs of all Divisions, Bureaux and Field Offices within the organization while ensuring that necessary governance mechanisms are in place and standards are adopted and adhered to.

The DIST organization is comprised of the CIO and Director's Office, and three primary Service areas, as shown in Figure 2.

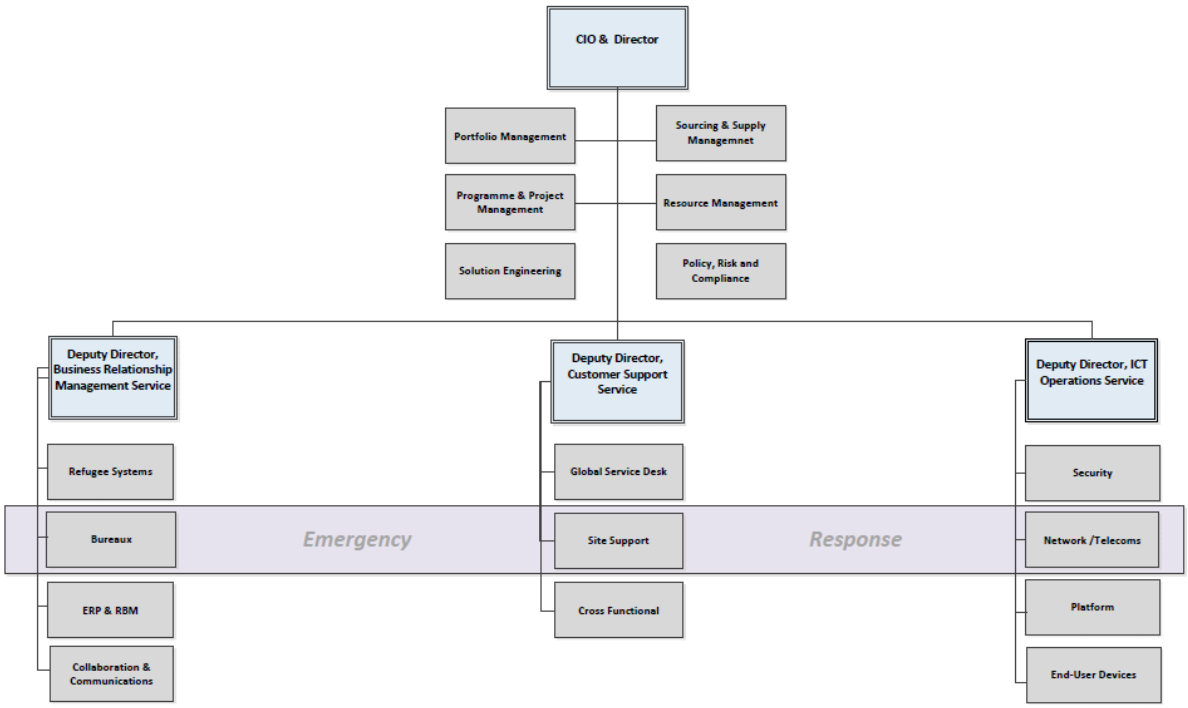

Figure 2 - DIST Organizational Structure

a) CIO & Director's Office

Led by the Chief Information Officer (CIO) and Director of DIST, this office is responsible for providing leadership and support in information and communication technology for UNHCR worldwide. The CIO is responsible for technology strategy and planning, performance and results, policy formulation, investment planning and oversight, project management, architecture and solutions engineering, compliance and audit coordination, supplier relationship management, and resource management.

The Director is supported by five sub-functions: (i) Resource Management; (ii) Sourcing and Supply Management; (iii) Portfolio Management Office (PMO); (iv) Solution Engineering; and, (v) Policy, Risk and Compliance.

b) Business Relationship Management Service

Led by the Deputy Director, Business Relationship Management (BRM), this Service is responsible for partnering with the Divisions and Bureaux who are the beneficiaries of DIST services to ensure that the services provided by DIST are fit for purpose and meet the ICT support needs of the organization. The staff members of the BRM Service focus specifically on building strategic partnerships with the Divisions and Bureaux which result in enhanced use of ICT to support and improve UNHCR's operations in the Field and in Headquarters.

c) Customer Support Service

Led by the Deputy Director, Customer Support Service, this Service has overall responsibility for the provision of quality ICT services to the UNHCR user community. The service liaises with external Managed Service Provider(s) to ensure an understanding of the requirements and that service delivery meets the agreed standards. The Customer Support Service includes the Global Service Desk, specific Site Support, and other Cross Function activities (i.e., change management, asset functions and configuration management).

d) ICT Operations Service

Led by the Deputy Director, ICT Operations, this Service has overall responsibility to design, deliver and maintain the common ICT Infrastructure which is the foundation of all services provided globally by DIST. This service covers the underlying Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) offerings provided via external third parties and UNHCR's Infrastructure and Communications Managed Services Providers. Located primarily in Amman, Jordan, the Service manages the operational (day-to-day) interaction with the various service providers through the service delivery management process. The Service also provides support to both infrastructure and applications projects through participation of its staff resources in the various project teams, in the provisioning of ICT infrastructure in support of the projects, and in the coordination of all related changes to common ICT infrastructure.

2.3 ICT Cybersecurity at UNHCR

2.3.1 Current Status

UNHCR activities are unique and decentralized. With operations in 130 countries, it features users with a mix of corporate and personal computing devices and with multiple entry points to connect to the network, all of which increases the difficulty to ensure robust ICT Security in a fast-moving environment where the priority is given to fieldwork due to its emergency characteristics.

UNHCR's system and network administration is mainly outsourced to third parties. The responsibilities of the ICT Security team, led by the Chief Information Security Officer – based in Amman, Jordan under the Deputy Director, ICT Operations – primarily cover security

governance, the establishment of security awareness program and the development and implementation of security policies to promote security good practices across the organization.

At the moment, the ICT Security team has limited tools and capacity to monitor external and internal environments in order to reliably detect any potential threats and malicious behavior. In addition, there is no Security Incident Event Management (SIEM) or Cyber Threat Intelligence (CTI) tools in place, nor is there centralization of security processes and technology in a Security Operations Center (SOC). For these reasons, there are no adequate event monitoring, log correlation, detection and response activities.

2.3.2 Challenges

In addition to the missing capabilities described above, some of the unique ICT Cybersecurity challenges facing UNHCR include:

- The distributed nature of UNHCR operations – with network bandwidth constraints, multiple WAN infrastructures, VSAT connection services and the overall dispersed nature of ICT resources – generates numerous connection points to UNHCR's network and to critical services/applications hosted at its data centers and in the cloud;
- A very flexible and mobile workforce – as well as non-staff partners – working in 130 countries, with a proliferation and continued used of corporate and personal mobile devices (laptops, smart phones, etc.);
- A variety of non-centralized applications at UNHCR field locations, which are not managed – or even always known by – the centralized DIST unit (aka "Shadow IT");
- The difficulty in effectively implementing ICT change across all operations in a timely manner, due to the distributed nature of the ICT landscape and to the operating model of UNHCR which prioritizes humanitarian emergency response;
- The specific needs of UN Jurisdiction and Immunities and Privileges, and the challenges of hosting of key services or data (such as PoC data) using "cloud" service delivery models;
- The increasing use of cloud services for commodity SaaS services such as Office365, as well as for PaaS and IaaS services such Azure and Amazon Web Services.

3 ICT Cybersecurity MDR Service Requirements

3.1 Services to be Provided

3.1.1 Service Description

UNHCR is seeking the support of a Service Provider to deliver Managed Detection and Response (MDR) services in support of UNHCR's ICT operations.

The key elements of the MDR service required by UNHCR are:

a. Remote managed, advanced end-point threat detection and/or malware protection and detection tools, delivered as a fully managed service, to be deployed across all UNHCR workstation and servers

b. Remote managed network IDS tools, delivered as a fully managed service, to be deployed at key network locations.

c. Where required, capacity to integrate and capture other system logs and event management data generated by selected UNHCR critical systems, network, and management and monitoring tools

d. Advanced capacity to aggregate, host, manage and retain all data collected from the above agents and tools, using vendor's owned and managed big-data platform

e. Retention of all relevant and detailed event data for each escalated incident, to be preserved until the resolution of incident itself;

f. Appraisal, filtering and/or aggregation of all relevant event data following the resolution of the incident, to be preserved for future forensic analysis, and to be transferred to UNHCR for archiving as a self-contained readable data package;

g. Advanced capacity to analyze and detect advanced threats, and capacity to target threat hunting and fine tune detection based on UNHCR's specific context in terms of operating model, applications and infrastructure

h. Provision and access to Advanced Threat Intelligence, including potential threats from state-sponsored cyber actors, and established and mature interaction with relevant Cybersecurity CERTs from governments and major ICT vendors

i. 24/7 monitoring and capacity to integrate with UNHCR ICT Operations processes and tools, as well as with those of UNHCR's major Managed Service Providers

j. Incident validation and immediate response capacity, through the provision of experts and account managers knowledgeable of UNHCR's environment in scope, readily available to assist UNHCR and MSP resources in the remediation of small to medium incidents

k. Establishment of an Incident Management Retainer to address and remediate major incidents, with expert resources readily available to complement and support UNHCR and MSP resources

l. Capacity to provide experts, on a daily or hourly basis, for the consulting and support of other cybersecurity projects, programs and major remediation activities

m. Periodic comprehensive reporting and participation in Program Management reviews with UNHCRs program management team

n. Capacity to provide reports as required including access to the contractors customer portal /dashboard to provide visibility of UNHCR's threat landscape, threat actors and remedial actions taken

o. Capacity to export actionable alerts to UNHCR's Security Operations Centre (when it becomes available) for incident resolution as required

3.1.2 Service Scope and volumes

For the scope of the evaluation of this RFP, the scope and service volumes will be the following:

- Advanced threat detection for 16,000 users, including their primary Windows workstations. A per-user based service subscription models would be preferred to allow the deployment of the end-point detection tool also on other critical end-user-devices used by the user
- Advanced threat detection for 2,500 servers
- 50 log feeds from critical systems or appliances
- 5 central UNHCR Network IDS points
- 500 hours of Incident Management Retainer per year
- 60 days of Cybersecurity expert consulting

4 Instructions for Bidders – Technical Proposal

Bidders who are interested in providing the ICT Cybersecurity Incident Managed Detection and Response Services described herein are requested to submit Proposals (with the associated commercial terms in Section 5) covering the areas described below.

The Technical Proposals will be evaluated in two main areas:

- Company Assessment
- Service Delivery Assessment

Please reply using the same section headings giving precise answers to the following questions.

4.1 Company Assessment

The Company assessment is based on the profile, financial stability, commercial experience, track record, reference accounts and development of human capital. The Bidder's ability to deliver the specified services and skills in a timely manner will be a major part of the assessment process.

4.1.1 Company Profile and Background

Provide the background of your company, including an overall summary experience relevant to the services requested as part of this RFP (more details will be requested starting in Section 4.1.3).

4.1.2 Financial Stability

The Proposal must outline long-standing history in the marketplace, a viable business model and continuously sound financial results. Please provide the following financial information:

- Summary financial statements (Operating Statement and Balance Sheet) for the last 3 years.

4.1.3 Relevant Experience

1. **ICT Cybersecurity Incident Managed Detection and Response Experience**

   Please describe your organization's specific ICT Cybersecurity Managed Detection and Response experience, including the following:

   a) Experience and examples of how you collect, manage and analyze cybersecurity big-data collected from endpoints, servers, appliances and logs deployed at customer premises

   b) Experience and examples of how you collect and manage Advanced Threat Intelligence

   c) Experience and examples of detecting and managing cybersecurity breaches and incidents originating from state-sponsored actors

2. **Relevant Environment Experience**

Please describe your organization's experience with the following:

a) Working on Cybersecurity incidents involving state-sponsored actors

b) Working with relevant Cybersecurity CERTs from governments and major ICT vendors

c) Working with large, complex, globally distributed organizations and customers

- Experience working with governmental and non-governmental organizations would be an asset.

- Experience with humanitarian programs and projects would be an asset.

d) Working and dealing with Cybersecurity incidents in regions such as Africa, Asia and the Middle East.

e) Experience with delivering MDR services across bandwidth-constrained and/or high-latency network environments.

4.1.4 Compliance Requirements

Please describe your organization's maturity and compliance in relation to attainment of relevant information security certifications.

a) This should include industry standard security certifications standards such as ISO 27001, SOC 2 and Cloud Security Alliance (CSA) or equivalent
b) Indicate the experience and relevant security certifications of staff members who may be assigned to this project

4.1.5 Customer References

Please provide at least three (3) detailed examples of customers for whom you have delivered major ICT Cybersecurity and/or Program Management services in the last five (5) years.

If applicable, please highlight in particular international organizations and/or UN organizations for which you have delivered these services.

Some areas of detail to include in each example (this is a non-exhaustive list, please provide additional information that you deem relevant) are:

a) What are/were the exact services provided?

b) What is the average size (revenue, number of devices, volume of data collected and analyzed, person days, details of profiles of resources allocated, etc.) and type of program?

c) How is/was the engagement structured and how did your staff engage with the customer staff?

d) Is/was the engagement successful? In what way did you measure success of the delivered services?

e) Is the engagement still on-going; if not, why not?

Please provide supporting information for each example, along with reference contact information. UNHCR reserves the right to contact these references without prior notification to the Bidder.

4.1.6 Global Reach

1. **Locations/Resources**

   UNHCR will require the services defined in this RFP to be delivered primarily remotely.

   In case on-site resources will be required, services will need to be delivered in Geneva, Switzerland and Amman, Jordan, but may exceptionally need to be delivered also in the other UNHCR headquarters (Budapest, Hungary and Copenhagen, Denmark) or any other field locations worldwide.

2. **Work Permits**

   While UNHCR will provide reference letters, the Bidder will be fully responsible for visa/permit applications. Repeated delays in having staff on-site due to visa/permit issues will be considered as grounds for termination of the Contract.

4.1.7 Relationship Management

Please describe how you develop and maintain strategic relationships, which provide added business value, reduced costs and increase your Advance Threat Intelligence. Provide at least one case study example.

Please provide details of strategic relationships with:

a) Governmental Cybersecurity organizations such as Intelligence or Law-Enforcement agencies

b) Major ICT Vendors such as Microsoft, Oracle, Amazon and others.

Please provide references for these strategic relationships. UNHCR reserves the right to contact these references without prior notification to the Bidder.

4.1.8 Security Procedures

The Service Provider's staff may have direct access to sensitive UNHCR information resources.

Please describe the programs, policies and procedures that you have in place for ensuring the protection of integrity and confidentiality of UNHCR information resources.

4.1.9 Uniqueness

Please indicate what distinguishes your company and/or your approach from other Bidders, and how this would benefit UNHCR. This is your opportunity to highlight qualities that are not covered in the other sections.

4.1.10 Additional Proposal Sections (optional)

In addition to the information specific to the service requirements, if desired please include additional information on alternative approaches that you believe will better meet UNHCR's Managed Detection and Response Service needs.

5 Instructions for Bidders – Commercial Proposal

5.1 Manner of submission

The manner of submission of the commercial proposal is outlined in the covering letter to this RFP.

5.2 Sales Engagement Process

The Proposal must outline the sales engagement process, including the following elements.

5.2.1 Contractual Terms

The Bidder is expected to accept UNHCR's standard "Terms & Conditions for the provision of Services" as provided as an Annex to this RFP.

5.2.2 Fee Structure and Price

Please note the following in preparation of your Bid:

1. The Service Provider is expected to provide the Contracted services:
    a. On a price per month per user and/or device, such as workstation, server, IDS appliance or log feed (Note that for end-user-devices, a per user/month pricing is preferred)
    b. On a price per hour for the Incident Management Retainer, based on a 500 hour per year baseline commitment and an hourly rate for additional hours.
    c. On a price per hour or day rate card for dedicated cybersecurity consultancy services, with a 60 day baseline per year and a daily rate for additional days
2. Specify the currency used. For comparison purposes, all amounts will be converted into US dollars using the prevailing UN rates of exchange.
3. The Proposal must outline the proposed Contract process including the typical terms under which resources are deployed.

Please note that the cost of the different components of the proposal is an important and influential factor of the bid and will be weighted accordingly. The specific costs should be set forth in the Commercial Proposal.

Please fill out the table provided as an Annex to this RFP and include the Excel spreadsheet in soft copy as part of the commercial proposal – DO NOT include this information in the technical proposal.

6 Additional information

6.1 Evaluation of Proposals

The process and deadlines for the RFP evaluation is outlined in the covering letter that accompanied this document. Please refer to and follow strictly the instructions in that letter. Failure to do so may result in your submission being eliminated or disqualified.

Your proposal will be evaluated from a technical and price perspective. Proposals that do not comply with the submission guidelines or which clearly do not meet the minimum technical requirements may be eliminated and not fully evaluated.

After the initial evaluation of materials provided, up to three (3) finalists will be identified and will be invited to give a face-to-face presentation of the submission to the evaluation panel. This presentation can be on-site in Geneva or via videoconference link.

6.2 Term of Contract

UNHCR anticipates entering into a Contract with the Service Provider for a term of three (3) years with an option to renew for two one (1) year periods (i.e., 3+1+1). Re-tendering can be expected at the end of the third year of the contract or prior to end of the third or fourth renewal term of the contract. The successful Bidder(s) should not assume that the contract will be renewed without retendering.

6.3 UNHCR General Conditions for the Provision of Services

UNHCR's General Conditions for the Provision of Services are included as an Annex to this RFP. By submitting a response to this RFP, you are indicating your agreement with those conditions.

Any Contract signed as a result of this RFP will be subject to the UNHCR General Conditions for the Provision of Services and any individual, consultant, or sub-contractor provided will also be bound to these General Conditions. These individuals will be expected to sign a declaration stating that their employer has made them aware of these General Conditions and any other specific clauses in the contract – in particular, the "declaration of confidentiality" clause.

6.4 UNHCR Special Conditions for Cloud Computing

UNHCR Special Conditions for Cloud Computing will be annexed to the agreement. Please review it and make comments if necessary.

6.5 UNHCR Special Data Protection Conditions

UNHCR Special Data Protection Conditions will be annexed to the agreement. Please review it and make comments if necessary.

6.6 UNHCR Vendor Registration Form

UNHCR's Vendor Registration Form is included as an Annex to this RFP. If your company is not already registered as a supplier to UNHCR please ensure that you complete this form and include it as part of the submission.

If your company completed the Vendor Registration Form before January 2010, you are requested to resubmit a completed form to show that you are aware of the revised General Conditions for the Provision of Services and accept them.

6.7 UN Supplier Code of Conduct

The UN Supplier Code of Conduct is attached as an Annex to this RFP. Any partner and their employees engaged with UNHCR will be expected to abide by this Code of Conduct.

6.8 Performance

Work is to be performed to the satisfaction of UNHCR. Performance and payment will be based on monthly management reports and approved individual time reports. There will be an implementation task for the Service Provider and UNHCR to jointly determine the methodology of the methods of measurement, the calculation of performance, and the preparation of regular reports.

UNHCR may require monthly performance reviews to include measurement satisfaction as well as service delivery. Bidders are invited to describe their approach to such reviews with particular reference to resolution of persistent problems, analysis of trends and plans for continuous service improvement.

The Service Provider will ensure that it and its personnel shall perform the Services with the necessary care and diligence, and in accordance with the highest professional standards. The Service Provider will be required to acknowledge and agree that it is entrusted with and has access to confidential and valuable information and data of UNHCR and that, with respect to such information, its will be held to the standard of care of a fiduciary. The services will be performed within the time limits established under the agreement. Where required by UNHCR with respect to particular deliverables, time will be of the essence and the parties will agree to liquidate damages for delay in performance.

UNHCR will have the right to review all work and services performed by the Services Provider. In the event of improper performance, UNHCR will have the right to require remedy by re-performance or other corrective measures. If such remedial measures are not promptly performed or if they fail to remedy the improper performance, UNHCR will have the right to engage third party entities, at the cost and expense of the Service Provider, to perform corrective measures.

6.9 Security Procedures

Non-UNHCR employees may have direct access to sensitive UNHCR information resources. The Bidder shall describe their programs, policies and procedures for ensuring the integrity and confidentiality of UNHCR information resources.

These policies and practices should include, but not be limited to, the following: managing OS access rights, managing passwords, Bidder procedures for their employee's departure, Bidder internal confidentiality agreements with their employees, security policies and practices related to remote management. Please provide a copy of the relevant portions of your Information Security Policy, Procedures, or Standards.

It is also a UNHCR requirement that all Service Provider employees engaged in work with UNHCR sign a Non Disclosure Agreement and the UN's Supplier Code of Conduct prior to commencement of any assignment.

UNHCR stores and processes large amounts of sensitive data about vulnerable individuals and takes very seriously its obligation to protect such data from unauthorized and improper

access, use, or dissemination The Service Provider will adhere to UNHCR's Policy on the Protection of Personal Data of Persons of Concern to UNHCR. In addition, as a UN agency and considering its status under international law, UNHCR will not enter into any contract that could jeopardize its position or infringe its privileges and immunities or compromise its rights to deny access to its data to any unauthorized individuals

- If the Service Provider will store POC personal data, it should be a requirement that the UNHCR Special Conditions for Cloud Computing are made part of the final agreement.

- If the Service Provider will be involved in processing POC personal data (even if stored on UNHCR controlled environments), then it should be a requirement that the UNHCR Special Data Protection Conditions are made part of the final agreement.

6.9.1 Business Recovery.

Please describe your business recovery plans.

6.10 Invoices

The selected Service Provider should submit monthly invoices covering the portion of the work that the Service Provider completed during the previous calendar month. Authorized time reports should be submitted with the invoices.

6.11 Payment Terms/Price Policy

6.11.1 Payment Terms

Fees under the Contract will be payable within 30 days of receipt by UNHCR of an invoice issued by the Service Provider, together with a certification by UNHCR that the work covered by the invoiced has been satisfactorily completed and any other documents (including timesheets, time accounting records and acceptance certificates certified by authorized UNHCR personnel) required by UNHCR.

UNHCR may withhold payment if, in the reasonable opinion of UNHCR, the Service Provider has not performed its obligations in accordance with the terms of the Contract. UNHCR and the Service Provider will consult in good faith to promptly resolve outstanding issues with respect to a disputed invoice. If UNHCR disputes an invoice, UNHCR will notify the Service Provider accordingly. Upon resolution of a dispute regarding an invoice, UNHCR will pay the relevant amount (if any) within 30 days from the date of resolution.

UNHCR will have the right, without prior notice to the MSP (any such notice being waived), upon any amount becoming due and payable hereunder to the Service Provider, to set-off any payment, indebtedness or other claim (including any overpayment made by UNHCR or any claim for loss or damage to UNHCR property) owing by the Service Provider to UNHCR hereunder or under any other agreement between the Parties. UNHCR will promptly notify the Service Provider of such set-off and the reasons therefore, provided, however, that the failure to give such notice will not affect the validity of such set-off.

The Service Provider will not be entitled to interest on any late payment or on any sums payable under the Contract, nor to any accrued interest on payments withhold by UNHCR that are subject to a dispute.

6.11.2 Service Level linked Payments

It is the intent of UNHCR to structure pro-rated payments based upon achievement of the agreed SLAs. It is also the intent of UNHCR that such prorated payments should decrease with consecutive months of non-attainment of SLAs.

6.12 Travel and Missions

It is possible that in completing the tasks specified that the consultants engaged under the terms of this Contract will need to travel to other locations (e.g. other UNHCR duty stations) in addition to being located in Geneva and/or Amman (as applicable). In this case, UNHCR will arrange and cover the costs of any such travel. The contractor will be entitled to the same DSA (Daily Subsistence Allowance) as UNHCR staff traveling to the same location. The Service Provider will be responsible for any travel authorizations (visas) and vaccinations as may be necessary. However, UNHCR will assist to the best of its ability in acquiring visas and medical clearance.

Any travel requirements will be clearly defined before the terms of the SOW are agreed to ensure that the staff provided for the engagement are available and eligible to travel.

6.13 Instructions on completing the spreadsheets

Two spreadsheets have been provided as an attachment to this RFP. Please follow the instructions in each for completing them.