CyberSouth
Cooperation on cybercrime
in the Southern Neighbourhood

Version 19 July 2018

# Situation report

## on specialised cybercrime and computer forensic units in Hashemite Kingdom of Jordan

Prepared within the framework of the
CyberSouth Project

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

**List of abbreviations**

| | |
|---|---|
| **CCCU** | Cyber Crimes Combating Unit |
| **CID** | Criminal Investigation Directorate |
| **ECRI** | European Commission against Racism and Intolerance |
| **ECTEG** | European Cybercrime Training and Education Group |
| **NAT** | Network address translation |
| **NICASS** | National Information Assurance and Cyber Security Strategy |
| **NCSS** | National Cyber Security Strategy |
| **PSD** | Public Security Department |
| **VOIP** | Voice over IP |

# INDEX

# 1 Introduction

## 1.1 Description of CyberSouth[1] project

Countries of the Southern Neighbourhood region, like any other country in the world, are confronted to the challenges of increasing dependency of our societies on information and communication technologies such as cybercrime. It is therefore essential for these countries to reinforce their institutional capacities to address cybercrime at country level, regional level and international level. Through the CyberSouth project, the European Union and the Council of Europe, in cooperation with other partners, will support this effort on the basis of existing tools and instruments including the Budapest Convention on Cybercrime.

**PROJECT OBJECTIVE AND EXPECTED RESULTS**

Objective: To strengthen legislation and institutional capacities on cybercrime and electronic evidence in the region of the Southern Neighbourhood in line with human rights and rule of law requirements

Result 1 - Criminal law frameworks strengthened in line with the Budapest Convention on Cybercrime, including rule of law safeguards (Article 15)

Result 2 – Specialised police services and interagency as well public/private cooperation strengthened

Result 3 – Judicial training on cybercrime and electronic evidence mainstreamed

Result 4 – 24/7 points of contact are operational (at prosecution and/or police level) for more effective international cooperation on cybercrime and e-evidence

Result 5 – Strategic priorities on cybercrime and electronic evidence identified

## 1.2 Aim of the report

The aim of this report is to make an analysis overview of the current situation on cybercrime and electronic evidence in the Hashemite Kingdome of Jordan by focusing mainly on:

- the state of the threat;
- the institutions responsible;
- training capacities and
- international cooperation.

The report summarizes the situation under each field, with some findings and action proposals.

The success of the project depends on a multiplicity of factors, including commitment by all actors, therefore some recommendations have been addressed at the end of the report at the attention of Jordanian authorities, the Council of Europe as well as some proposals to the European Union.

[1] The exact name of the project according to the delegation agreement concluded between the Council of Europe and the European Union (ENI/2017/385-202) is Cybercrime@South.

## 1.3 Collection of information

Following the Workshop on Responses to the challenge of Cybercrime on 05 March 2018 Jordanian authorities accepted to welcome a Council of Europe delegation to evaluate the anti-cybercrime capabilities in Jordan, within the framework of the CyberSouth project on 04-06 June 2018.

The Jordanian Armed Forces facilitated the organisation of the meetings with the judiciary gathering representatives from the Ministry of Justice, as well as from the Public Security Department.

The Council of Europe delegation was composed of:

- Adrian LAMBRINO, Head of Combating Organised Crime Brigade Ploiesti, National Police, Romania;
- Zahid JAMIL, Barrister, Consultant on cybercrime and electronic evidence, Pakistan;
- Marie AGHA-WEVELSIEP, Project Manager for CyberSouth, Council of Europe;
- Ionut STOICA, Senior Project Officer for CyberSouth, Council of Europe.

The delegation was welcomed by Jordan authorities who confirmed their willingness to cooperate in this project and especially expressed the need for capacity building on cybercrime. Jordan has already strong capacities in the fight against cybercrime through strong political will supported by other European funded projects.

# 2 Overview of cybercrime

Jordan has a population of 7 million with 87.8% of internet users. Among internet users, 89% use Facebook, 71% use WhatsApp, 66% use YouTube, 43% use Google Plus and 34% use Instagram[2]. Smartphone penetration is at 87%[3].

## 2.1 State of the threat

The number of reported crimes related to the use of computer systems has increased. According to the Public Security Department (PSD), in 2008 only dozens of crimes were recorded and in 2017, this increased to 5200 cases. Most of reported crimes committed are identity and data thefts, man in the middle cyber-attacks, defamation and threats on social media, embezzlement, credit cards fraud and cases related to intellectual property and child abuse via Internet.

Within the framework of the project on "Strengthening the capacity of the Public Administration to combat Cyber Crime in the Hashemite Kingdom of Jordan" funded by the European Union and implemented by United Kingdom in partnership with the Czech Republic, a baseline assessment report was produced in 2014. The report referred to a list of crimes investigated by the Cyber Crimes Combating Unit (CCCU) which remains still valid in 2018: electronic fraud, threatening, blackmailing and defamation through social media, hacking of websites, theft of data and information, online money laundering, theft of credit cards credentials, hacking of e-mails, sexual exploitation/child exploitation, impairing or hindering services and websites, editing or changing the database of some corporations, publishing and hosting pornography, online forgery of documents, cheques or credit cards and using them, misleading advertisements, blackmailing and threatening through phone, fraud through SMS, theft of mobile phones and illegal use of VOIP.

Most cybercrime reported are cyber enabled crimes, there are very little crimes reported against technology itself, only 200 cases of data theft in 2017 were reported.

**Statistics.** There are some statistics for cybercrime or offences involving electronic evidence in law enforcement and also in the judicial system (MISAN). MISAN is a court case processing system which enables the collection of statistics on cybercrime and electronic evidence cases. The PSD is considering reviewing classification of cybercrime and electronic evidence related cases.

**Reporting system mechanism.** Complaints may be submitted directly to the police stations, through the 911 emergency call, via email (psd@psd.gov.jo ), on Facebook account of the Cyber Crimes Combating Unit (CCU) or to the public prosecutor's office. Crimes reported via email or Facebook should be followed up by an official complaint at the police station or the public prosecutor office in order to be registered as such.

## 2.2 Cybersecurity and cybercrime strategies

### 2.2.1 Cyber security strategy

In 2012, Jordan adopted a National Information Assurance and Cyber Strategy[4] (NIACSS) which aims primarily at protecting the national IT infrastructure. NIACSS has set up five strategic objectives that range from preventing attacks to critical information infrastructures, reducing vulnerabilities, minimizing damage and recovery to increasing confidence and trust in information systems and information security awareness.

[2] http://www.jordantimes.com/news/local/facebook-whatsapp-overshadow-twitter-jordan%E2%80%99s-social-media-sphere
[3] https://thearabweekly.com/jordan-sounds-alarm-over-rising-online-crimes
[4] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/jordans-national-cyber-security-strategy

In February 2018, the Ministry of Information and Communications Technology published the National CyberSecurity Strategy (NCSS) under the National CyberSecurity Programme for public consultation. NCSS aims to review the progress made since NIACSS and establish new priorities for the next five years.

Among key successes of NIACSS, the establishment of a national cyber academy to create a cyber-security awareness and capacity building programme is to be highlighted. This demonstrates the importance for Jordanian policy makers in growing national expertise in the field of cybersecurity.

The NCSS[5] is focussed on the following four strategic objectives:

- "to protect, enhance the trust in and resilience of the Government, Critical National Infrastructure businesses and the general public against cyber threats;
- to detect hostile action against Jordan and its information assets;
- to respond to cyberattacks in the same way other attacks on national security are responded to;
- to evolve and develop the knowledge, skills and sustainable sovereign capability required to maintain robust cyber security".

With respect to its implementation, the NCSS is to be implemented by the Higher CyberSecurity Council. The Higher CyberSecurity Council will be chaired by a senior official of the Government but shall also have representatives from defence and security, financial critical network infrastructure and the private sector.

### 2.2.2 Cybercrime strategy

At the state level there is no policy or strategy regarding cybercrime. Since cybersecurity is mainly dedicated to the protection of critical information infrastructure (CIIP), cybercrime measures provide a criminal justice approach to attacks against the confidentiality, integrity and availability of computer data and systems. Thus, if both cybersecurity and cybercrime are complementary in the case of attacks against computer data and systems, they follow a different rationale. Therefore, a cybercrime strategy that addresses prevention and criminal justice policies should be considered to address the full range of cybercrime issues. Issues to be considered in this respect should be[6]: cybercrime reporting and intelligence, prevention, legislation, high-tech crime and other specialized units, interagency cooperation, law enforcement training, judicial training, public-private cooperation, effective international cooperation, financial investigation and prevention of fraud and money laundering and protection of children.

The baseline report of the project on Strengthening the capacity of the Public Administration to combat Cyber Crime in the Hashemite Kingdom of Jordan had already mentioned the need to adopt a cybercrime control strategy to reduce threats created by cybercrime. The final report of the project dating from 5 April 2015 reiterates as part of the recommendations the need to "create key policy and strategic documents such as serious crime strategy, intelligence strategy, cybercrime strategy and threat assessment."

CyberSouth project could be an opportunity for Jordan to assist with the creation and implementation of a cybercrime strategy.

[5] moict.gov.jo/uploads/Public-Consultations/NCSS-DRAFT.pdf

[6] http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e1

### 2.2.3 Findings and proposals

**Findings.** Police statistics and governmental CERT statistics offer information to help in the evaluation of cyber threats. The cybersecurity strategy of Jordan is in force and it has effective results. The absence of cybercrime strategy might impede to have a persistent approach in the fight against cybercrime and in the cooperation between actors responsible for cybercrime and cybersecurity.

**Activities proposals.** CyberSouth project could facilitate the organisation of one regional event and one national event on reporting system mechanism and on the need to elaborate a cybercrime strategy along with an action plan. Any activity in that sense should be to complement what has been already implemented by Jordanian authorities since the final report of the project on "Strengthening the capacity of the Public Administration to Combat Cyber Crime".

# 3 Legal framework on cybercrime and electronic evidence

At this stage, Jordan did not request to be invited to accede to the Budapest Convention.

The provisions regarding the validity of electronic documents are introduced in **Electronic Transaction Law No. 15 of 2015.**

## 3.1 Legislation on cybercrime and electronic evidence

The Electronic Crimes Law No. 27 of 2015 (Electronic Crimes Law) is the cybercrime legislative framework of Jordan. Jordan is in the process of updating the Electronic Crimes Law to keep up with the continuous evolution of cybercrime and the threats posed by criminal actors in the cyberspace.

**Substantive provisions**. Articles (3) to (12) of the Electronic Crimes Law provide substantive law on offences against the confidentiality, integrity and availability of computer systems and computer data, as well as computer-related offences and content-related offences.

**Procedural provisions**. Article (13) of the Electronic Crimes Law provides for procedural and investigative powers with respect to offences committed under the Electronic Crimes Law. In particular, Article (13) enables judicial police to enter into any location in which has been used to commit an offence under the Electronic Crimes Law and search any "devices, hardware, software, operating systems, information system, and means" that evidence shows were used to commit such offences, with prior permission and keeping in consideration third-party rights. Separately Article (13C) also empowers the competent court to order the judicial police to seize any "devices, tools, means, and materials" used to commit an offence under the Electronic Crimes Law with prior permission. Competent courts also have the additional power to order hinder the operation of an information or website that is used to commit an offence. However, the Electronic Crimes Law does not provide for any other key procedural powers to obtain electronic evidence.

**Sanctions**. It was observed by most stakeholders that existing punishments/sanctions related to the offences in the Electronic Crimes Law were very low and were not effective deterrence for cybercriminals. The Ministry of Justice and the Legal Committee have proposed to enhance existing sanctions under the law and also criminalize certain conduct that is not criminalized. For instance, the amendments attempt to criminalize computer-related forgery, hate speech, and embezzlement. While this appears to be a step in the right direction, there is still certain conduct (i.e. Computer-related forgery) that has not been addressed.

## 3.2 Protection of children against online sexual violence

Jordan does not have any specific legislation for the protection of children against online sexual violence. The Law No. 32 of 2014 concerning Juvenile Law ("Juvenile Law") provides for the protection of children generally, though an English copy of this legislation was not made available.

The Electronic Crimes Law No. 27 of 2015 articles 9 & 15 includes provisions on hotline reporting service for incidents of online sexual violence against children in Jordan.

## 3.3 Responsibilities of Internet service providers

Telecom Regulatory Commission of Jordan (TRC) has issued regulations that require its ISP licensees to retain data including NAT logs for a period of two years.
According to authorities, law enforcement based on agreements with ISPs is able to obtain traffic data and subscriber information directly from ISPs. Public Security Department get the authorization of the prosecutor to obtain data from the ISPs.

## 3.4 Regulations for the financial sector

The Central Bank of Jordan has a Memorandum of Understanding with other official bodies in Jordan to provide data on cybercrime attacks that target both the Central Bank of Jordan and other banks. Under the Jordanian banking law, all banks and financial institutions are required to report any incidents (including cybercrimes or any other errors that affect operations) within a period of 72 hours. Banks however are not required to report any incidents involving passwords, PINs or social engineering directly affecting consumers, or any incident involving the general ledger of the bank itself.

If a bank fails to report an incident, it may be fined a maximum of USD 100,000. The Consumer Protection Department of the Central Bank of Jordan has devised a four-part manual form for reporting incidents, which includes information about bank, details about the attack/attacker, time of attack and controls or measures taken to remediate. Phishing attacks are reported daily, therefore they imposed to the banks to have two types of authentication.

The Central Bank of Jordan has played a proactive role in creating awareness about cybercrime for banks, employees and customers. It was learned that the Central Bank of Jordan is also looking to establish a FINCERT which would also respond to cyber incidents involving banks and financial institutions in Jordan.

## 3.5 Other regulations addressing cyber-related emerging threats

In 2014, the Central Bank of Jordan issued instructions prohibiting local banks, financial institutions, payment processors and currency exchangers from dealing with crypto currencies. There are however no specific regulations regarding virtual currencies. Though citizens are not prohibited from trading in crypto currencies or organizing ICOs, the Central Bank of Jordan has warned consumers about associated risks. Jordan has issued no regulations with respect to other emerging threats such as illegal activities on the Dark Web.

# 4 Institutional capacities in the fight against cybercrime

The authorities dealing with cybercrime are the General Prosecutor's Office and the Public Security Directorate (PSD) within the Criminal Investigation Department (CID) with the Cyber Crimes Combating Unit (CCCU) who has some cross competences with other police units.
Within Public Security Directorate, there is a section called Family Protection Department which is dealing with child abuse cases.

## 4.1 Judiciary

Article 97 of the Constitution ensures the independence of the Judiciary: "Judges are independent, and in the exercise of their judicial functions they are subject to no authority other than that of the law."

There are three categories of courts:
- Civil Courts
- Religious Courts
- Special Courts

**Role and capacities of prosecution services.** The General Prosecutor's Office has a special prosecutor's unit responsible with serious cyber cases only.
Members of the CCCU assist the prosecution service and play a proactive role with regard to the prosecution of cybercrime cases in particular. The absence of a sufficient number of specialized prosecutors for cybercrime and electronic evidence cases is highlighted as a challenge.

## 4.2 Law enforcement: specialized units on cybercrime and computer forensic units

**Specialised unit.** The specialized body dealing with cybercrime is Cyber Crimes Combating Unit (CCCU). This unit started in 2008 as a section called CID Cyber Crime Section and developed during the time, in pace with the trends of the criminality, until 2015 when the section was reinforced and upgraded to the unit level.

There are also specialized units in every region of the country. In cities where there are no specialized cybercrime units the complaints may be submitted at the local Criminal Investigation Departments which has police officers trained as first responders for such cases.

The number of cases related to cybercrime is increasing every year starting from 48 cases in 2008 until 5487 cases in 2017.

**Cooperation with ISPs.** CCCU cooperates with ISP's by mutual agreements. Warrant from prosecutors is needed to obtain the data from the ISP's. There is also a good cooperation with the financial providers Western Union and Money Gram who have local branches and deliver quick answers. CCCU has also a good cooperation with the Central Bank of Jordan and the Anti-Money Laundering Unit.

**Prevention.** CCCU conducted awareness raising campaigns including on their Facebook account. The unit organized on-line workshops, targeting college and university students, especially on cyber bullying topics. Those workshops where attended by 650.000 students. The unit also made more than 780 prevention presentations through all over the country, in universities and they also participated on meetings at national television regarding cyber awareness

**Forensic capabilities**. A Forensic Laboratory Department (FLD) was created within PSD in 1998 responsible for forensic recovery and analysis of digital evidence from various devices.
In 2010, a Digital Evidence Laboratory (DEL) was established within CCCU which consists 5-6 officers. The officers attended several training sessions with U.S. specialists. The number of requests goes up to 5000 devices every year. There is a standard operating procedure for cybercrime investigations and for handling electronic evidence.
CCCU offers support to other investigation units in cases involving online investigations and dealing with electronic evidence.

## 4.3 Computer Emergency Response Team (CERT)

For the moment there are two CERTs in Jordan, one for the Government and also one for the Jordan Armed Forces. There is a project for developing a CERT for Public Security Directorate in the future.

The governmental CERT consists of 20 positions and for the moment only 10 of them are occupied. They are not doing international cooperation, which is made only through Jordan Armed Forces CERT.

There is no cooperation procedure between government CERT and ISP's. Traffic data and subscriber information data are retained for two years. There are some procedures in place to handle incidents. Currently, the governmental CERT is receiving information about illegal activities from other state agencies.

## 4.4 Findings and activity proposals

### 4.4.1 For law enforcement

**Findings.** The CCCU and DEL need more physical space to carry out their daily tasks. CCCU does not have suitable premises for victims to fill in complaints and to carry out investigation. The same observation can be applied for the Digital Evidence Laboratory. Also, it is not clear if regional CCCU do have the same capability as the central CCCU.

**Recommendations.** CCCU and DEL should be further developed to allocate sufficient physical space for ensuring work quality environment. Renewal of licensed programs used by the DEL and the CCCU should be managed through a long-term strategy that would include increase of knowledge in using open source programs and strategic use of licensed standard software (Encase Forensic and others).

**Activity proposals**. In order to strengthen specialised police services and interagency as well public/private cooperation, the following activities are suggested:

- A regional activity on defining a strategic approach and an action plan on cybercrime to better identify and assess threats and propose the appropriate measures.
- Study visit to a European Cybercrime Unit – for learning about the best practices from other European countries
- Workshop on International cooperation with the ISPs
- Advisory mission on standard operating procedures for cybercrime investigations and for handling e-evidence (chain of custody)

# 5 Law enforcement training

At the Royal Police Academy there are courses dedicated to cybercrime investigation. In most of the cases, training is provided to law enforcement by foreign entities such as European Police College (CEPOL) and Federal Bureau of Investigations from USA.

Each officer from CCCU has taken multiple courses on cybercrime. A number of 30 officers from CCCU are trainers for other police officers for first responder courses. The training program was provided by UNODC. Usually, officers from this unit held courses to the audience composed of more than 300 prosecutors and judges.

The previous programme on Strengthening the capacity of the Public Administration to combat Cyber Crime in the Hashemite Kingdom of Jordan contributed to develop a first responder guide and a first responder course.

## 5.1 Findings and recommendations for law enforcement training

**Findings.** Even though training activities on cybercrime are conducted, there is no strategy for law enforcement training on cybercrime and electronic evidence. It has not been possible to establish the number of law enforcement agents with first responder capacity and the number of cybercrime investigators and their training level.

**Recommendations.** An action plan dedicated to training needs on cybercrime should be developed at the level of PSD to help to increase knowledge within CCCU and also share the knowledge gained at the regional level. This would also help to have a more systematic approach and better use funds available by external donors to grow local expertise instead of relying only on external supports.

**Activity proposals.** CyberSouth project works in cooperation with European Cybercrime Training and Education Group (ECTEG) and could offer the possibility to benefit from the following range of training used by European law enforcement agencies:

- Live data forensic
- Dark web investigation basic and crypto-currencies
- Malware analysis
- Online open source investigation (OSINT)
- E-learning on first responder course

The trainings proposed are falling within a specific strategy that is to create local expertise on the long term. These trainings will be regional and thus number of places available is limited. Therefore, it will be the responsibility of management to determine the most skilled staff to take part in trainings with the capabilities to further disseminate them internally.

# 6 International cooperation on cybercrime and electronic evidence

**Police to police cooperation.** Cooperation is mostly done via Interpol channel. There are no laws governing such cooperation. An average of 200 requests are sent out and 100 are received for police to police cooperation related to cybercrime every year. There is no specific procedure for emergency requests.
Law enforcement in Jordan also cooperates informally with service providers outside Jordan, though the police have difficulty obtaining evidence from certain providers. Law enforcement often obtains and provides court orders providing basis for such cooperation. In addition, law enforcement in Jordan also cooperates directly with foreign law enforcement agencies and share information spontaneously.

**Judicial cooperation.** Jordan does not have any specific legislation enabling international legal cooperation or mutual assistance in general but there are several articles in several laws on this matter. However, authorities are engaging in international cooperation on the basis of multilateral and bilateral treaties.

Any requests that are received through the Ministry of Foreign Affairs and Expatriates are sent to the central authority within the Ministry of Justice. All requests are considered internally by the Judicial Council and a legal opinion is prepared on whether the request fulfils all legal requirements. Once approved by the Ministry of Justice, the request is referred to the First Public Prosecutor of Amman to initiate an investigation and collect the subject evidence. The results of the investigation will be shared with the Attorney General of Amman for assessment as to whether the investigation is satisfactory. Upon the approval of the Attorney General of Amman, the results of the investigation are sent to the Ministry of Justice which transmits it onwards through the Ministry of Foreign Affairs and Expatriates.

# 7 Recommendations and proposals

## 7.1 Recommendations to Jordanian authorities

In order to use the resources of the project effectively, Jordanian authorities are invited to:

- To facilitate the nomination of project team members to implement the project representing each institution: Ministry of Justice, Prosecution, Public Security Department (CCCU and DEL), Judicial Institute/Judicial Council and Police Training Institute. A focal point should be nominated to coordinate with all relevant institution the implementation of the project;
- Set up a formalized mechanisms for cooperation between the private sector and Jordanian authorities (CERT, Police Units or Judiciary).
- To facilitate access to legislation, regulation or circulars related to cyber and electronic evidence;
- To communicate the necessary information to the Council of Europe to conduct studies and researches;
- To express needs for training in a clear and targeted manner so that the setup of training reach expectations and meet the needs of Jordanian authorities;
- To take ownership in the organization of in country activities;
- To nominate the appropriate representatives for participation in different project events.

## 7.2 Recommendations to the Council of Europe

The Council of Europe will endeavor the necessary efforts to build a relation of trust with Jordanian authorities essential for a successful implementation, and in this regard commits:

- not to disclose any information related to Jordan without the prior authorization of the project team;
- to support Jordanian authorities in their process of reforms on cybercrime and electronic evidence.

# 8 Appendix

## 8.1 Agenda and list of interviews

Version 25 May 2018

**Assessment visit**

Amman, 4-6 June 2018

**Draft Programme**

| Date | Time | Meetings |
|---|---|---|
| 4 June 2018 | 11.00 -14.00 | **Judicial training institution** http://www.jij.gov.jo/ |
| 5 June 2018 | 11.00 -14.00 | **Cyber Crimes Unit(PSD)** |
| 6 June 2018 | 11.00 -14.00 | **National Information Technology Center** http://www.nitc.gov.jo/ |

**List of interviews**

**4 June meeting**

Judge Ammar Husseini, Judicial Council
Judge Ali Al-Musaimi, Judicial Council
Abdullah Abu Al-Ghanam, Amman District Prosecutor, Judicial Council, judge_abdullah@yahoo.com
Major Judge Yarob QUDAH, Directorate of CyberSecurity & Information Technology/JAF, yarobqudah@yahoo.com
Ola. M. Obeidat, Judicial Institute, ola.obeidat@moj.gov.jo
Ahmad SARRAWI, Head of Technical Support Section, Judicial Institute, ahmad.sarrawi@moj.gov.jo
Lt. colonel Ashraf Karaimeh, Head of National Cyber Security Project Development Branch, Directorate of CyberSecurity & Information Technology/JAF, a.karaimeh@jaf.mil.jo

**5 June meeting**

Representative of PSD
Head of CID
Head of CCCU
Lt. Wesam AL-ZYOUD, Head of Internet Crimes Section, Public Security Department, wesam.alzyoud@psd.gov.jo
Captin Mahmoud Maghaireh cyber.crimes@psd.gov.j

**6 June meeting**

Representative from the Central Bank of Jordan
Representative from CERT