CARICOM CYBER SECURITY AND CYBERCRIME ACTION

one space• one Caribbean

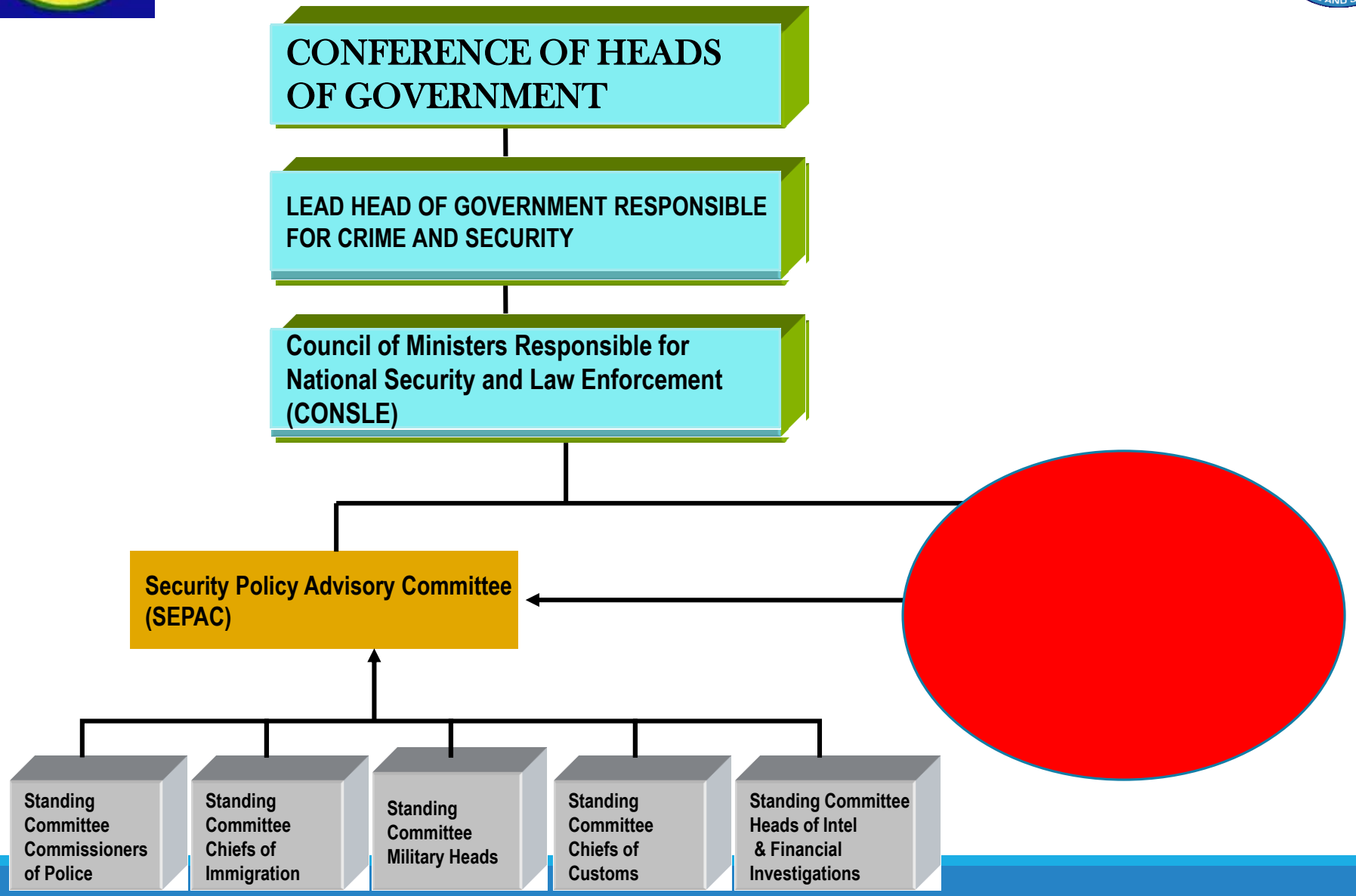
Presented by: -
Sean Fouché
Information Communication Technology Manager

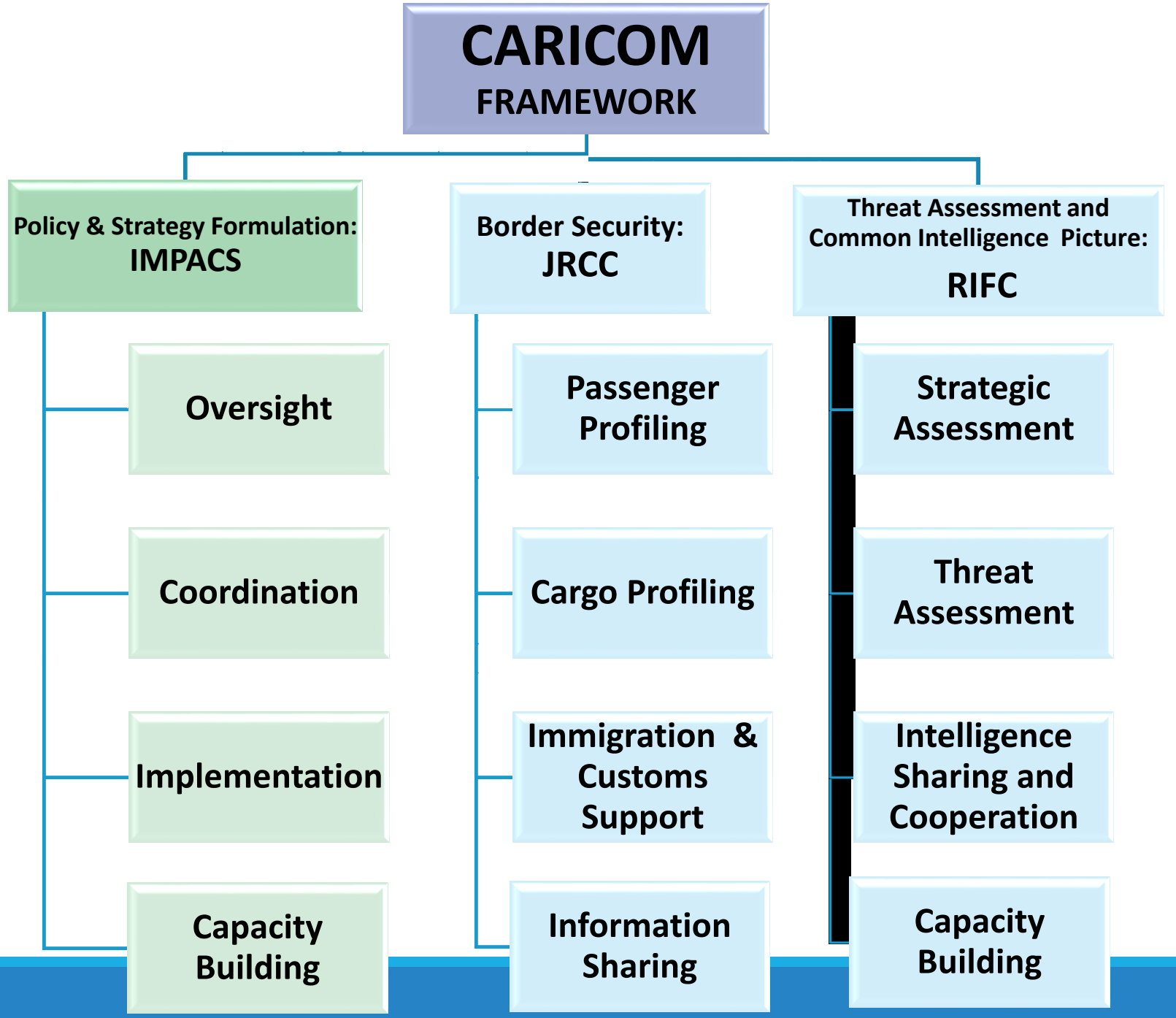
Agenda

- Introduction to CARICOM IMPACS
- CARICOM Crime and Security Strategy (CCSS)
- Cyber Security and Cybercrime in CARICOM
  - Focus
  - Initiatives
  - Moving Forward - Action Plan

CARICOM STATES

CARICOM FRAMEWORK FOR THE MANAGEMENT OF CRIME AND SECURITY JULY 2005 AND AMENDMENTS (2012)




CARICOM
FRAMEWORK
Policy & Strategy Formulation:
IMPACS
Oversight
Coordination
Implementation
Capacity Building
Border Security:
JRCC
Passenger Profiling
Cargo Profiling
Immigration & Customs Support
Information Sharing
Threat Assessment and Common Intelligence Picture:
RIFC
Strategic Assessment
Threat Assessment
Intelligence Sharing and Cooperation
Capacity Building

Regional Threat Perspective
Current Realities

- **Narcotics and Arms Trafficking**
- **Human Trafficking**
- **Violent and Organized Crime**
- **Irregular Migration**
- **Terrorism**
- **Cyber Crimes**
- **Criminal Deportees**

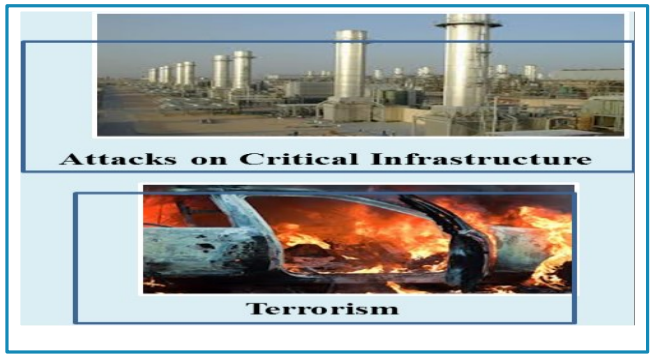
CARICOM Crime and Security Strategy (CCSS)

- Adopted at the 24th Inter-sessional meeting of the conference of Heads of Government of CARICOM – February 2013
- Goal - to significantly improve citizen security by creating a safe, just and free Community, while simultaneously improving the economic viability of the Region.
- Identifies and prioritises the common security risks and threats which CARICOM is facing now, and are likely to face in the future
- Articulates an integrated and cohesive security framework to confront these challenges
- Guides the coordinated internal and external crime and security policies adopted by CARICOM Member States, under their respective legal frameworks.

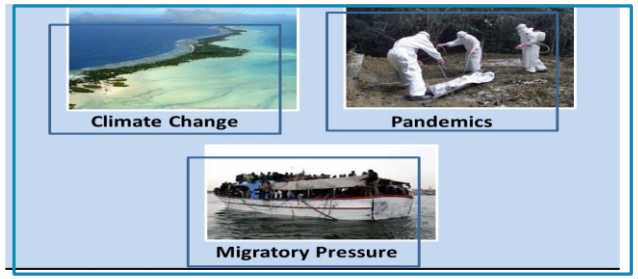
CARICOM Crime and Security Strategy: Tiers

Tier 1: Immediate Significant Threats:
high-probability, high-impact events

Tier 2 : Substantial Threats:
both likely and relatively high-impact



Tier 3: Significant Potential Risks:
high-impact, but low-probability



Tier 4: Future Risks:
Uncertainty in the probability and impact

CARICOM Crime and Security Strategy (CCSS)

Identifies four (4) tiers of risks/threats which are common to CARICOM Member States as follows:-

- ❑Tier 1 – Immediate Significant Threats: Transnational Organised Crime, Gangs and Organised Crime, Cyber Crime, Financial Crimes, Corruption
- ❑Tier 2 – Substantial Threats: Human Trafficking and Smuggling, Natural Disasters, Public Disorder Crimes
- ❑Tier 3 – Significant Potential Risks: Attacks on Critical Infrastructure, Terrorism
- ❑Tier 4 – Future Risks: Climate Change, Pandemics, Migratory Pressure

TIER 1: IMMEDIATE SIGNIFICANT THREAT

Transnational Organised Crime: Trafficking of Illicit Drugs and Illegal Guns

Gangs & Organised Crime

Cyber Crimes

Financial Crimes

Corruption

CARICOM Crime and Security Strategy (CCSS)

According to the CCSS - STRATEGIC GOAL #8 – **Strengthen CARICOM's Resilience to Cyber Crime** - Enhancement of CARICOM's resilience to cyber security threats through a comprehensive **Regional Cyber Security Strategy**

- Capacity Development,
- Policy and Legislative Strengthening
- Effective Response Mechanism Strengthening

Strategic Plan for the Caribbean Community

- In the Strategic Plan for the Caribbean Community 2015-2019, Cybercrime is listed as an obstacle and threat to social and economic development in CARICOM.
- Strengthening cybersecurity is seen as a strategy to achieve technological resilience but is also linked to strategies needed to achieve social resilience and citizen security.

CARICOM IMPACS – CYBER INITIATIVES

- The CARICOM Crime and Security Strategy, adopted at the Twenty-Fourth Inter-sessional Meeting of the Conference of Heads of Government of CARICOM, in February 2013, Cybercrime is listed under the "Tier 1 – Immediate Significant Threats" with strategic goal 8 being "Strengthening CARICOM's Resilience to Cyber Crime".
- In the Strategic Plan for the Caribbean Community (CARICOM) 2015-2019, Cybercrime is listed as an obstacle and threat to social and economic development in CARICOM. Strengthening cybersecurity is seen as a strategy to achieve technological resilience but is also linked to strategies needed to achieve social resilience and citizen security.
- Single ICT space – CARICOM IMPACS has responsibility for Cyber Security and Cybercrime initiatives

CARICOM IMPACS – CYBER INITIATIVES

- The first Caribbean Stakeholders' Meeting (CSM I) held in Trinidad and Tobago in May 2014, served to raise awareness of the potential impact of Cybercrime and was convened by the Commonwealth Secretariat and supported by the CTU, OAS/CICTE and CARICOM IMPACS.
- At the CTU 25th Anniversary ICT Week held in February 2015 the issue of Cyber Security and Cybercrime was again highlighted and in this case the meeting reviewed and updated the Caribbean Cyber Security Framework, which was developed by the CTU and the OAS in 2012

CARICOM IMPACS – CYBER INITIATIVES

- The second Caribbean Stakeholders' Meeting (CSM II) convened by the Commonwealth Secretariat and supported by the CTU, OAS/CICTE and CARICOM IMPACS held in Saint Lucia in March 2016, was designed to build on the previous initiatives and to develop a comprehensive Action Plan for Cyber Security and Cybercrime in the Caribbean
- At CSM II CARICOM IMPACS was identified as the lead implementation agency for Cyber Security and Cybercrime in the region.
- CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) – lead by CARICOM IMPACS when finalised will be presented to CONSLE for approval

CARICOM IMPACS – CYBER INITIATIVES

- Global Crisis Response Support Programme (GCRSP)
  - Development of the human resource capacity of IMPACS, RSS, CDEMA and CARPHA in areas related to crisis monitoring and management
  - Assistance in the design and development of protocols for crisis monitoring and management activities and initiatives for each Regional Agency and regional collaborating mechanisms for detection and prevention and monitoring of crisis
  - Assistance in the development of joint crisis response plans and protocols for regional agencies and stakeholders
  - One of the main areas of concern identified was that of ***Cybercrime***

CARICOM IMPACS – CYBER INITIATIVES

- GCRSP project and CARICOM and the OAS
  - Enhancement of Media Monitoring capability for CARICOM through technical support from the OAS
  - Collaboration on Cyber with the OAS/CICTE Unit

- **Cyber Security training**
  - To increase capacity of regional agencies
  - To assist in cementing IMPACS' role as the coordinating actor for cyber security in CARICOM
  - The programme was a good forerunner to planned work in cyber security in the CARICOM region in the near future

CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP)

Areas to be addressed: -

- The establishment of a Regional Cyber Committee;
- The identification of minimum standards for Cyber Security for each country;
- An updated (desk) status review of each country;
- Identification of mechanisms for implementation of the relevant action items - Common Needs, Solutions and agencies/partners with interest (present or potential**)**; and
- Monitoring and evaluation of activities to ensure that objectives are being achieved.

CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP)

Priority Areas - Common Needs, Solutions and agencies/partners with interest

1. Public awareness;
2. Building sustainable capacity;
3. Technical standards and Infrastructure;
4. Legal Environment; and
5. Regional and International Cooperation Collaboration - Incident response, cybercrime investigation and capacity building.

QUESTIONS

Thank you