NATO COMMUNICATION AND INFORMATION SYSTEMS GROUP

Mons - Belgium

NCISG/J3/2022/0312

26 September 2022

TO: See Distribution

SUBJECT: **CALLING NOTICE FOR STEADFAST COBALT 23 (STCO23) FIRST TEST MANAGEMENT WORKSHOP (TMWS1), 17-21 OCT 2022**

REFERENCE: Exercise Specification for Exercise Steadfast Cobalt 2023 (Draft).

1. This letter and enclosed documents are the calling notice for the First Test Management Workshop (TMWS1) of the Exercise STCO23.

2. In accordance with the eMTEP, STCO23 is planned to be executed from Peace Time Locations (PTL), from 11 Apr to 05 May 2023 (Phase IIIB Execution). The Officer Scheduling the Exercise (OSE) is SACEUR, and the Officer Conducting the Exercise (OCE) is the Commander of the NATO CIS Group (NCISG).

3. In accordance with EXSPEC, it is foreseen to conduct three TMWSs. The focus of the first TMWS will be to familiarize all units with the test content as well as finalizing the scope, objectives and number of test scenarios. The Evaluation Group (EG) will develop technical, procedural and organizational EVAL aspects.

4. The first TMWS will be held from 12:30h on Monday 17 October 2022 to 12:00h Friday 21 October 2022 all within the NCI Agency, The Hague Facility. The draft agenda is in ANNEX A where a detailed time schedule per service can be found and detailed info for the different sessions.

5. The expected attendees are the lead SME for services, test coordinators from the NATO Force Structure (LCC, MCC, ACC, SOCC, CBRN, US EUCOM, CATF/CLF, EUROCORPS. MND SE, JTFHQ, JLSG) Units, Test Management Team Lead, Interoperability Director/Deputy and Test Directors and Deputies to STCO23. Furthermore, all members of the STCO23 Evaluation Group (EG) are requested to attend the Evaluation syndicate. There is a specific request to have testers from NCISG NSB's that are involved in the CIS security testing to attend the TMWS.

6. Participants from the NATO Command structure (AIRCOM, LANDCOM, MARCOM, NSHQ, SHAPE) are require to send an individual request for participation to the Points of Contacts within this calling Notice. This is due to the limited amount of space available within the NCI Agency facility during this meeting.

NCISG
7010 Mons, Belgium
Office : +32 65 443998
Mobile : N/A

NCN 254-3998
Fax : +32 65 443854 (Registry)
david.koblizek@ncisg.nato.int

7. All participants are expected and requested to register online at the internet web site: https://cvent.me/XXQMEa. Please see links on CVENT site for access information/ security, parking, public transport, electronic equipment, luggage, food &beverage and local accommodation suggestions. Please pay specific attention on security and electronic equipment details as some of the planned meeting rooms are in the Class II area, NCIA cannot afford to assign personnel to accompany persons that need an escort during the conference. Make sure you acquire unescorted access.

8. The Points of Contact for the meeting are:

- Test Management Syndicate
  - Mr. Andres Bulk
  - Tel: +31 70 374 3448 (NCN 257 3072)
  - Email: andres.bulk@ncia.nato.int

  - Mr. Werner Slippens
  - Tel: +31 70 374 3699 (NCN 257 3699)
  - Email: werner.slippens@ncia.nato.int

- Evaluation Syndicate
  - JFCBS J6 DIREVAL OPR, Piotr Straton
  - Tel: NCN 244 3352
  - Email NS/NU: Piotr.Straton@jfcbs.nato.int

FOR THE COMMANDER NATO CIS GROUP:

Egbert FIKOWSKI
Colonel, DEU Army
Acting Chief of Staff

ANNEXES:

A. TMWS-1 Agenda
B. The Hague Security requirements (PSC)
C. NCI Agency Electronic devices Policy

DISTRIBUTION:

External:

Action:

AIRCOM
ARRC (NFS LCC for NRF 2024)

BICES Group Executive (BICES NSHQ)
EUROCORPS (for J2C2 2024)
ESP JFAC (NFS ACC for NRF 2024)
ITA MARFOR (NFS MCC for NRF 2024)
JALLC
JFCBS
JFCBS JLSG
JFCNP
JFCNP JLSG
JSEC
JWC
J6 FMN Secretariat
LANDCOM
MARCOM
MNC NE
MND NE
MND S
MND SE
NAEW&CF HQ
NCI Agency (as Service Management Authority and Technical Authority for NRF 2023)
NHQC3S
NMR of Estonia to SHAPE (for NFIU and as FMN Affiliate)
NMR of France to SHAPE (for CATF and CLF as NRF 2024 and as FMN Affiliate)
NMR of Germany to SHAPE (for 1* stand-down BDE and as FMN Affiliate)
NMR of Hungary to SHAPE (for NFIU and as FMN Affiliate)
NMR of Italy to SHAPE (for ITA MARFOR as NRF24 MCC, for 1* stand-up BDE for NRF 2024, for NRDC-ITA, for MND-S and as FMN Affiliate)
NMR of Lithuania to SHAPE (for NFIU and as FMN Affiliate)
NMR of Latvia to SHAPE (for NFIU and as FMN Affiliate)
NMR of the Netherlands to SHAPE (for as FMN Affiliate)
NMR of Poland to SHAPE (for NFIU, MNC-NE, MND-NE, CBRN BN as NRF 2024, SOCC as NRF 2024 and as FMN Affiliate)
NMR of Romania to SHAPE (for MND-SE and as FMN Affiliate)
NMR of Slovakia to SHAPE (for NFIU and as FMN Affiliate)
NMR of Spain to SHAPE (for ESP JFAC, as NRF 2024 and as FMN Affiliate)
NMR of United Kingdom to SHAPE (for ARRC as NRF 2024, 1* stand-by BDE and as FMN Affiliate)
NMR of United States to SHAPE (for USEUCOM and as FMN Affiliate)
NSHQ
PNMR of Sweden
SACT
SHAPE CCOMC
SHAPE CyOC
SHAPE J2X (As security Accreditation Board Lead)
SHAPE J6 Cy

Information:

NMR of Albania to SHAPE (as FMN Affiliate)
NMR of Belgium to SHAPE (as FMN Affiliate)
NMR of Bulgaria to SHAPE (as FMN Affiliate)

NMR of Canada to SHAPE (as FMN Affiliate)
NMR of Croatia to SHAPE (as FMN Affiliate)
NMR of the Czech Republic to SHAPE (as FMN Affiliate)
NMR of Denmark to SHAPE (as FMN Affiliate)
NMR of Greece to SHAPE (as FMN Affiliate)
NMR of Iceland to SHAPE
NMR of Luxemburg to SHAPE (as FMN Affiliate)
NMR of Montenegro to SHAPE (as FMN Affiliate)
NMR of North Macedonia to SHAPE
NMR of Norway to SHAPE (as FMN Affiliate)
NMR of Portugal to SHAPE (as FMN Affiliate)
NMR of Slovenia to SHAPE (as FMN Affiliate)
NMR of Türkiye to SHAPE (for MJWC, for TUR JFAC and as FMN Affiliate)
SHAPE Partnership Directorate

Internal:

Action:

J1
J4
J2/6
J3
1 NSB
2 NSB
3 NSB

Information:

J5
J7
J8
LEGAD
HSI

ANNEX A: TMWS-1 Agenda

Date: Monday 17th OCT							
TIME		Security	COI	CORE	ENABLING	JISR	EVALUATION
Room		E3 160.5	E3 251	F3 450	F3 430	F3 400	E3 160.4
0900-1000		Arrival	Arrival	Arrival	Arrival	Arrival	Arrival
1000-1030							
1030-1130		Arrival	Arrival	Arrival	Arrival	Arrival	Arrival
1130-1230		Lunch	Lunch	Lunch	Lunch	Lunch	Lunch
1230-1330		F1-380 (MCR)	F1-380 (MCR)	F1-380 (MCR)	F1-380 (MCR)	F1-380 (MCR)	F1-380 (MCR)
1330-1430		CIS Security combined session	AIRC2	Digital Certificates	Audio & Video	JISR	Eval
1430-1530		CIS Security combined session	AIRC2	Data Directory Synchronization	Audio & Video	JISR	Eval
1530-1630		CIS Security combined session	Battle Space Events	Data Directory Synchronization	Audio & Video	JISR	Eval

Date: Tuesday 18th OCT							
TIME		Security	COI	CORE	ENABLING	JISR	EVALUATION
Room		E3 160.5	E3 251	F3 450	F3 430	F3 400	E3 160.4
0900-1000		CIS Security POL SOCC	Data Links	Formal Messaging	Audio & Video	JISR	Eval
1000-1030							
1030-1130		CIS Security POL CBRN	Data Links	Formal Messaging	Audio & Video	JISR	Eval
1130-1230		CIS Security ARRC	Joint Targeting	Informal Messaging	Audio & Video	JISR	Eval
1230-1330							
1330-1430		CIS Security ESP JFAC	Joint Targeting	Informal Messaging	Communications	JISR	Eval
1430-1530		CIS Security ITA MARFOR	Land C2 Info Exchange	Informal Messaging	Communications	JISR	Eval
1530-1630		CIS Security FRA CATF/CLF	Land C2 Info Exchange	Informal Messaging	Communications	JISR	Eval

Date: Wednesday 19th OCT							
TIME		Security	COI	CORE	ENABLING	JISR	EVALUATION
Room		E3 160.5	E3 251	F3 450	F3 430	F3 400	E3 160.4
0900-1000		CIS Security NCISG *(preferred testers from NSB's)*	Friendly Force Tracking	Web Authentication	Communications	JISR	Eval
1000-1030							
1030-1130		CIS Security NCISG *(preferred testers from NSB's)*	Logistics	Web Authentication	Communications	JISR	Eval
1130-1230		CIS Security Spare	Logistics	Web Authentication	Communications	JISR	Eval
1230-1330							
1330-1430		CIS Security Spare	Missile Defence	Web Authentication	Domain Naming	Geo Spatial	Eval
1430-1530		CIS Security Spare	Operations Planning	Web Authentication	Domain Naming	Geo Spatial	Eval
1530-1630		CIS Security Spare	Operations Planning	Web Authentication	Domain Naming	JISR	Eval

Date: Thursday 20th OCT							
TIME		Security	COI	CORE	ENABLING	JISR	EVALUATION
Room		E3 160.5	E3 251	F3 450	F3 430	F3 400	E3 160.4
0900-1000		No program	Recognized Maritime Picture	Web Hosting	Domain Naming	JISR	Eval
1000-1030							
1030-1130		No program	Recognized Maritime Picture	Web Hosting	Domain Naming	JISR	Eval
1130-1230		No program	Situational Awareness	Web Hosting	Domain Naming	JISR	Eval
1230-1330							
1330-1430		No program	Situational Awareness	Web Hosting	Distributed Time	JISR	Eval
1430-1530		No program	Text Based Collaboration	Web Hosting	Distributed Time	JISR	Eval
1530-1630		No program	Text Based Collaboration	Web Hosting	Distributed Time	JISR	Eval

Date: Friday 21th OCT							
TIME		Security	COI	CORE	ENABLING	JISR	EVALUATION
Room		E3 160.5	E3 251	F3 450	F3 430	F3 400	E3 160.4
0900-1000		No Program	CBRN	Workflow	Spare	JISR	Eval
1000-1030							
1030-1130		No program	Time Sensitive Targeting	Spare	Spare	JISR	Eval
1130-1230		No program	Time Sensitive Targeting	Spare	Spare	JISR	Eval
1230-1330							

Meeting Rooms Secure Area				
E3 251 (NS)	E3 160.4 (Class II)	E3 160.5 (Class II)	F1-380 (MCR)	
24 Pax	12 Pax	12 Pax	109 Pax	

Meeting Rooms Admin Zone		
F3 400	F3 430	F3 450
14 Pax	14 Pax	14 Pax

ANNEX B: The Hague Security Requirements

CONTROL OF ACCESS ARRANGEMENTS FOR NCI AGENCY, THE HAGUE

The NCI Agency Building is divided in an Administrative Zone and Class II Security Area.
All visitors are required to produce a valid NATO Security Pass/ID card or a valid Passport/National photographic Identity Card, as proof of identity. In addition:

Administrative Zone:

To attend a NATO UNCLASSIFIED or NATO RESTRICTED meeting in the administrative zone:
NATO UNCLASSIFIED, no further Security clearance details are required.
NATO RESTRICTED, if not in possession of a valid PSC, you are required to sign a "Certificate of Security Obligation" which is required in order to allow you access to NATO RESTRICTED information.
The appointed NCI Agency POC / Sponsor for the meeting is responsible for co-ordinating these requirements as part of the meeting arrangements/preparation.

Class II Security Area:

For UNESCORTED access to the NATO Class II security area or to attend a NATO CONFIDENTIAL and above event, please note the following:

A validated NATO SECRET or COSMIC TOP SECRET Personal Security Clearance (PSC) is required.

How to provide proof of NATO PSC:
- Military and Civil servants from NATO entities (ACO, ACT, NATO HQ or Agencies): on arrival produce an AMIS card or security pass which is subject to a reciprocal agreement with NCI Agency (those with a AMIS Card please put your AMIS Card number into your Cvent registration for validation). On arrival your valid reciprocal badge will be exchanged for a local unescorted visitors pass.

- Military and Civil Servants from NATO nations: submit proof of their NATO Secret security clearance by submitting Request For Visit through the appropriate National Security Authority (NSA) or a Personnel Security Clearance Confirmation (PSCC) through their Facility Security Officer (FSO) to thehague.security@ncia.nato.int. The PSCC template is available in APPENDIX 2 to ANNEX 1 to AC/35-D/2000-REV8 Dated 25 Nov 2020.
Please note: Attestations of Personnel Security Clearance are no longer the accepted document, being replaced by PSC confirmations in NATO Security Policy (NSP) in November 2020 and are now the approved format to be used.

- **Visitors from Industry**: Your FSO (Facility Security Officer) should submit a Request For Visit (RFV) to validate the visitor(s) NATO PSC through their National Security Authority (NSA). RFV forms should be available from your FSO or NSA.

- **For USA Visitors from Industry**: Your FSO should submit an RFV as proof of the visitor(s) NATO PSC through DCSA. DCSA contact details and further RFV completion details can be found at https://www.dcsa.mil/mc/ctp/int/visits/

In the RFV submission, please use the following POC for Security:
•NAME: Mr. Robin Bell
•E-MAIL: thehague.security@ncia.nato.int
•TELEPHONE NO: 0031 70 374 3222

ON ARRIVAL
- Subject to proof of validated NATO PSC being presented on arrival or having been forwarded in advance, and a valid photographic identity document, visitors will receive an UNESCORTED Visitor's Pass. If no validated proof of NATO PSC is provided, visitors will be ESCORTED at all times by a nominated sponsor. If the event is NATO CONFIDENTIAL or above, access will be denied.

To attend a NATO RESTRICTED event
- To allow UNESCORTED access to the Class II Security Area and to be able to access NATO RESTRICTED information, a NATO PSC is required (to be provided in accordance with the arrangements detailed above). Those without a NATO PSC will be ESCORTED and required to sign a `Certificate of Obligation' to allow them to access NATO RESTRICTED information.

To attend a NATO UNCLASSIFIED event
- To allow UNESCORTED access to the Class II Security Area, a NATO PSC is required (to be provided in accordance with the arrangements detailed above). Those without a NATO PSC will be ESCORTED.

Non-NATO Nations/Entities
- If you are from a non-NATO NAtion or Entity, then please contact the thehague.security@ncia.nato.int for further information.

Contacts:
Email: thehague.security@ncia.nato.int
NS WAN: Search for ** NCIA – Security Services The Hague or email NCIA-SecurityServiceTH@ais.nato.int
Email CC :
Roy.Molegraaf@ncia.nato.int
William.Burndred@ncia.nato.int
Dennis.VanDerLinden@ncia.nato.int

ANNEX C: CIS EQUIPMENT/MEDIA GUIDANCE

The following provides direction on the use of Mobile Communication Devices, including (but not limited to) portable computers, smartphones, smart watches, wearable devices, tablets and laptops, with internet, Bluetooth, transmitting, positioning (eg GPS), camera and/or recording capabilities and/or media by visitors to NCI Agency The Hague (TH), The Netherlands.

• Mobile Communication Devices, including portable CIS, may only be introduced to / used in NATO Class II security areas if they are NATO/NCI Agency owned or managed devices, or specifically authorised following assessment of justification for official work by NATO/NCI Agency authorities, this includes contractor owned CIS in support of official work.

• An application prior to introduction of CIS / Mobile electronic devices must be made with a full justification from the visitor and visit sponsor stating the operational/business criticality of the requirement and the operational/business impact of refusal to permit access. Application forms can be obtained from visit sponsors and/or NCI Agency TH security.

• Use of camera, telephone and/or recording features on the equipment is strictly prohibited.

• Equipment may only be used in a stand-alone mode (except when connecting to the Agency's Public Guest Network).

• The visitor must have had the equipment under their personal control since it left its permanent location and ensure that the equipment remains under their control at all times. If the visit is for more than one day, the visitor is strongly advised to secure the equipment in an appropriate office in NCI Agency TH outside of normal working hours (if at all possible).

• The equipment and its associated computer storage media, must be protected at all times in accordance with the security regulations applicable to the highest classification level of information stored or processed.

• NATO Security Policy forbids staff to accept and upload any data provided on media from any outside source before such media has been checked for viruses. Storage media associated with a portable computer brought from the outside should normally be used only on that equipment. If there is a requirement for controlled exchange of information, special security arrangements should be agreed in advance between the staff concerned, the NCI Agency TH IT Helpdesk, NCI Agency TH CIS Security Manager and the NCI Agency TH Site Security Manager.

• The connection of non NATO/NCI Agency Equipment to any NCI Agency CIS network is prohibited (with the exception of NCI Agency's Public Guest Network – if available).

Use in NCI Agency TH Conference Rooms

• Mobile Communication Devices approved for access to NCI Agency TH may only be used in a conference room with the approval of the Chair of the Committee/Working Group. However, if allowed, they must be accredited in terms of being able to process classified information at the same level as the meeting. Mobile Telephones and Electronic Devices with SIM cards
• Use of such devices is not permitted by visitors (i.e. non-NCI Agency Staff/Consultants) and must be stored in the lockers provided or left in your vehicle/hotel room.

THIS IS A GUIDE ONLY AND IS NOT EXHAUSTIVE. APPLICATIONS MUST BE RECEIVED BY NCI AGENCY TH SECURITY AT LEAST 5 WORKING DAYS IN ADVANCE OF THE VISIT. PLEASE ADDRESS ANY QUERIES IN RESPECT OF THE ABOVE TO NCI AGENCY TH SECURITY: thehague.security@ncia.nato.int