

**NOTE BY THE TECHNICAL SECRETARIAT****WORK OF THE INVESTIGATION AND IDENTIFICATION TEAM
ESTABLISHED BY DECISION C-SS-4/DEC.3 (DATED 27 JUNE 2018)**

1. The Conference of the States Parties (hereinafter “the Conference”), at its Fourth Special Session, adopted a decision entitled “Addressing the Threat from Chemical Weapons Use” (C-SS-4/DEC.3, dated 27 June 2018). In paragraph 10 of C-SS-4/DEC.3, the Conference decided that the Technical Secretariat (hereinafter “the Secretariat”) shall put in place arrangements to identify the perpetrators of the use of chemical weapons in the Syrian Arab Republic by identifying and reporting on all information potentially relevant to the origin of those chemical weapons in those instances in which the OPCW Fact-Finding Mission (FFM) determines or has determined that use or likely use occurred, and cases for which the OPCW-UN Joint Investigative Mechanism (JIM) has not issued a report; and that the Secretariat shall provide regular reports on its investigations to the Executive Council (hereinafter “the Council”) at its regular sessions and to the United Nations Secretary General, for their consideration.
2. In this context, at its Twenty-Third Session, the Conference adopted the Programme and Budget of the OPCW for 2019 (C-23/DEC.10, dated 20 November 2018), which takes into account resource requirements for implementing paragraph 10 of C-SS-4/DEC.3.
3. The Council at its Ninety-First Session received a Note by the Secretariat entitled “Work of the Investigation and Identification Team Established by Decision C-SS-4/DEC.3 (dated 27 June 2018)” (EC-91/S/3, dated 28 June 2019) informing all States Parties about the establishment of the OPCW Investigation and Identification Team (IIT) with the purpose of identifying, in compliance with C-SS-4/DEC.3, perpetrators of the use of chemical weapons in the Syrian Arab Republic.
4. The IIT, as an integral part of the Secretariat and functioning under the authority of the Director-General, has started its investigatory work. Beginning in May 2019, it has developed and implemented a system to establish the focus of its investigation, thus formulating a non-exhaustive preliminary list of nine incidents it would focus on. It has further prepared its investigation plan and is currently implementing it.
5. During the past months, the IIT has reached out to States Parties and other international, regional, and local actors in order to gather information and conduct investigations and analysis, as it considers necessary and appropriate, including with respect to access to victims and witnesses or other sources of information. In order to establish proper communication and cooperation channels, in particular with entities



other than States, the IIT operates on the basis of general principles of cooperation aimed at protecting the confidentiality of sources and information, as required, and at ensuring the integrity of the process of information gathering.

6. IIT activities include gathering and assessing information provided to it by OPCW States Parties and other international, regional, and local actors as well as, where applicable and relevant, examinations and analyses seeking to identify the origin of the chemical used, munition markings and physical characteristics, and technical information and/or extrapolations related to delivery means, such as aircraft flight paths or munition trajectories. The activities also include interviews with victims and other witnesses of the incidents, with experts in the various subjects relevant to the investigation, and evaluation of open-source material. In fulfilment of its mandate, the IIT collects and analyses information and material from any relevant source in addition to those already obtained by the FFM, also in order to determine the relevance, probative value, and reliability of the information, as well as the credibility of the source. The IIT has further commenced reviewing and analysing the information it is obtaining, so as to properly categorise, assess, and evaluate it. In the event that new or emerging analysis techniques can assist the IIT, subject matter experts will be consulted to advise the IIT on the applicability of the methods as they pertain to the IIT investigation.
7. During its activities, the IIT resorts to technical assessments and scientific evaluations with the aim of providing an overall description of incidents, patterns, and the origin of any chemical weapons used in the incidents considered, endeavouring to identify perpetrators on the basis of a predefined degree of certainty. Before making findings, the IIT shall duly take into account all available information, including that provided by the Syrian Arab Republic as well as by others, on the hypotheses and scenarios considered by the IIT.
8. In order to proceed with its independent investigations in an objective and impartial manner, the IIT has further developed internal work practices, further to consultations within the Secretariat, in particular relating to information management, investigations and evidence collection, documentation, and chain of custody. In general, since the activities of the IIT require vast amounts of information to be collected and created, seamless and robust procedures are required to allow for the secure, consistent, and transparent management of information, from its collection or creation through its ultimate preservation, transfer, or destruction. In setting up the regime, confidentiality and security requirements deemed necessary for the storage and use of the information material provided by other entities were taken into account.
9. Overall, the IIT aims at ensuring the security, integrity, preservation, and chain of custody of the information and material in its possession from the moment of receipt, collecting, analysing, and storing technical and scientific information meeting the highest technical standards, as well as the meticulous employment of forensic processes. Access to information within the IIT is on a need-to-know basis. Effective

and secure information handling is considered a key factor for the IIT to fulfil its mandate by:

- (a) ensuring the safety and security of the IIT's activities, personnel, and third parties;
 - (b) maintaining the integrity of its records and evidence;
 - (c) ensuring effective and timely search, analysis, and dissemination of information; and
 - (d) increasing the awareness of confidentiality requirements by promoting correct information handling practices.
10. Established internal work practices related to information management cover all kinds of information material (comprising records and evidence) created, received, and managed by the IIT, which may include both digital and physical records. Provisions are made to ensure confidentiality of both categories in terms of organisational, physical, and information security measures.
 11. In particular, and in addition to organisational and physical arrangements, all of the IIT's information management systems and its file storage system reside in the IIT Secure Network (ISN), designed and built in compliance with the OPCW Security Critical Network policies and requirements for OPCW confidential material. The ISN is accessible by designated terminals possessing appropriate security and confidentiality measures, which are "air gapped" and therefore separated, with no network interface.
 12. IIT work practices provide for the registry procedure, the structure of the central repository for the IIT's records and evidence, access permission based on roles, responsibilities, the repository's contents, as well as the retention schedule of IIT records and information. Such practices ensure that the chain of custody of information and the audit trail of records are properly captured, in order to ensure the continued integrity and authenticity of evidence. The IIT has developed, and continues to monitor, its own workflow to manage information, including creating, receiving, transmitting, reproducing, scanning, printing and sharing records by external storage devices, email, shared drives, and team sites. The IIT has further implemented steps to protect, and capture results from, open-source searches directly related to the identification of perpetrators within the IIT mandate.
 13. The IIT has decided to implement, within the ISN, an investigation management system to support investigation activities. This investigation management system is meant to capture investigation and analysis activities to ensure the authenticity and reliability of records. The system, accessible through specific encrypted terminals in the ISN, is thus designed to allow the IIT to securely keep the records and evidence associated with investigation and analysis activities, add relationships between records and evidence, and provide feedback on investigation steps. All electronic information collected and generated by the IIT as a result of its investigation activities will be stored in the evidence management system, which is also designed to capture the purpose for and modalities in which records are collected, so as to enhance their

evidentiary value. The documentary physical records will be scanned and saved in the system, unless a different procedure is required in light of the nature of the record.

14. Access control functions in the investigation management system allow IIT personnel to access records with specific predefined permissions (including permissions to create, read, modify, and delete records). To ensure that no records of the IIT are deleted from the system or lost, only pre-authorised IIT personnel are able to delete records. The system further provides for audit trails that cannot be modified or removed. IIT personnel are trained in the use of the system as required and maintain awareness of the necessary security and confidentiality measures taken to protect the information material.
15. As the work of the IIT progresses, a backup plan is being implemented in order to enhance security.
16. The IIT welcomes input from States Parties, and relies on cooperation pursuant to paragraph 7 of Article VII of the Chemical Weapons Convention (hereinafter “the Convention”), in particular with the provision of relevant information and access to relevant places and persons. Further to EC-91/S/3, the Director-General, during his opening statement to the Council at its Ninety-First Session, requested all States Parties concerned to provide their full cooperation to the IIT (paragraph 21 of EC-91/DG.25, dated 9 July 2019). In September 2019, communications requesting assistance were sent to all States Parties, reiterating calls for assistance and specifically requesting information potentially relevant to establish the origin of the chemical weapons used in the nine identified incidents and useful to identify perpetrators (including delivery methods and background information related to actors that might have the capabilities to use such weapons), evidence suggesting or contradicting attribution to certain actors, as well as any element related to the relevance, probative value, and reliability of such information, as well as the credibility of sources.
17. The IIT is in the process of preparing a first report on certain incidents under its consideration, to be provided consistent with paragraph 10 of C-SS-4/DEC.3, to the Council for its consideration.
18. This Note regarding the work of the IIT established by C-SS-4/DEC.3 is hereby circulated for the information of States Parties to the Convention.

--- 0 ---