OPCW

Technical Secretariat

Verification Division
S/1192/2014
1 July 2014
Original: ENGLISH

NOTE BY THE TECHNICAL SECRETARIAT

SECURE INFORMATION EXCHANGE (SIX)

Introduction

1. Timeliness of exchange of information between the States Parties and the Technical Secretariat (hereinafter "the Secretariat") is crucial for the effective and efficient implementation of the Chemical Weapons Convention (hereinafter "the Convention").

2. The information exchanged between the States Parties and the Secretariat may contain both classified and unclassified information. In the case of classified information, the only authorised mechanism currently available for the transmission of such information is the physical exchange of information via the authorised representatives of the States Parties. In most cases, the information is transmitted via diplomatic pouch from the capitals to the authorised representatives, who then hand-deliver this information to a representative of the Secretariat. This process imposes logistical difficulties that can cause delays and may, therefore, adversely impact the timely fulfilment by the States Parties of their obligations under the Convention, such as the timely submission of declarations, as well as important activities of the Secretariat, such as the evaluation of declarations and the planning of inspections.

3. To address this issue, in 2012 the Secretariat initiated the secure information exchange (SIX) project, with a view to establishing an end-to-end process that would enable the secure electronic exchange of information between States Parties and the Secretariat.

4. The Secretariat continued to develop the SIX project in 2013, and the system will be ready for use in July 2014. It will be available to all interested States Parties that wish to utilise the system as an alternative mechanism for secure communication with the Secretariat.

Background

5. The timely submission of declarations required under Articles III and VI of the Convention and relevant Parts of the Verification Annex of the Convention is of utmost importance for the implementation of the verification regime established by the Convention. Any improvements to the efficiency and quality of the relevant transmission processes are directly linked to the performance of the OPCW's core objectives. While the timeliness of declarations has been improving over time, a

significant number of declarations are still received late, and one of the most frequently cited reasons for missing the submission deadlines is related to "logistical difficulties in regard to the transmission of declarations to the Secretariat".[1] Such difficulties stem primarily from the fact that, regardless of whether they are in hard copy or in electronic format, the declarations are transmitted from the National Authorities to the Permanent Representations of States Parties to the OPCW via diplomatic pouch and physically handed over to the Secretariat. This process inherently requires time, which may entail delays and adversely affect the timeliness of submission of the declarations. These "logistical difficulties" may persist in the absence of an appropriate framework and a corresponding technical system enabling the National Authorities of the States Parties to transmit declarations electronically through a secure channel.

6. In addition, there is a comparable need for a secure channel for transmission of other documents that contain confidential information (such as reconciliation reports, clarification and transfer discrepancy letters, and relevant responses), which are exchanged between the Secretariat and the States Parties on a regular basis. Occasionally the Secretariat receives confidential information via unauthorised means, for example, by post or in plain e-mail messages, which introduces security risks and may lead to unauthorised access to confidential information.[2]

7. The main objective of the SIX project was to define a process and provide a channel for the efficient and secure electronic exchange of information with minimal additional cost compared to traditional means of transmission (in hard copy or on CD-ROM), which also utilises existing infrastructure and established procedures.

8. The main beneficiaries of the new end-to-end process will be the States Parties, in particular the representatives of National Authorities who are directly involved in the implementation of the Convention, especially the preparation and submission of Article III and Article VI declarations. In addition, the Secretariat will also directly benefit from the anticipated efficiency gains and reduction of costs associated with the manual exchange of information, including in relation to Article III and Article VI declarations in the initial stages and, possibly in the future, in relation to other areas where similar needs are identified, such as for transfer discrepancies.

---

1 In accordance with the decision of the Executive Council on timely submission by States Parties of declarations under Article VI of the Convention (EC-51/DEC.1, dated 27 November 2007), the Secretariat reports regularly on the timeliness of submissions of declarations under Article VI of the Convention. The quotation is from the questionnaire that the representatives are requested to fill out and submit together with their delayed declarations. For the most recent report on timely submissions, see "Status Report on Timely Submission by States Parties of Declarations under Article VI of the Chemical Weapons Convention for the Period from 1 January to 31 December 2013", EC-75/DG.1, dated 15 January 2014.

2 In accordance with paragraph 3 of the Confidentiality Annex to the Convention, the Secretariat reports annually on the implementation of the regime governing the handling of confidential information. For the most recent report on this topic, see EC-75/DG.9 C-19/DG.2, dated 28 February 2014.

Status of SIX

9. In 2013, the Secretariat completed a feasibility study and subsequently presented the project to the Industry Cluster in two of its meetings.[3] Following the demonstration of the envisioned process to the Industry Cluster and the positive response received from the States Parties, the Secretariat continued with a pilot phase. Several States Parties participated in the pilot programme, which comprised establishment of software components, exchange of security keys used for encryption and decryption of information and, finally, the actual transmission of test documents.

10. The project and the findings from the pilot programme were shared with the representatives of the National Authorities who attended the Fifteenth Annual Meeting of National Authorities, held in The Hague from 27 to 30 November 2013. A demonstration of the end-to-end process was also provided in the margins of the Eighteenth Session of the Conference of the States Parties.[4]

11. The SIX system will be ready for use in July 2014 and available to those States Parties that wish to use it for the secure transmission of information to the Secretariat in relation to their Article III and Article VI declarations or for the receipt of the information from the Secretariat.

Using SIX

12. The use of SIX by States Parties is optional and it is within the discretion of States Parties to opt for the secure transmission of information to the Secretariat through this system or through more traditional means.

13. The use of the SIX system is subject to the acceptance of the terms and conditions set forth in Annex 1 of this Note both by States Parties, upon registration using the form contained in Annex 2 to this Note, and by their authorised representatives, upon access to the SIX Portal. Login to the SIX Portal will be through a secure dedicated link, and the authorised representatives of the States Parties will be required to accept the terms and conditions, which will be referenced on the home page of the SIX Portal.

14. Any State Party willing to receive from, and/or transmit to, the Secretariat information through SIX system must provide to the Secretariat the name, job title, telephone number, and e-mail address of up to two authorised persons designated by the Government of that State Party for such purposes, so that the Secretariat can appropriately identify and authenticate each user of SIX. To ensure a higher level of security for communication and the exchange of information through the SIX system, the Secretariat advises States Parties to provide institutional or governmental e-mail addresses rather than generic or web-based free e-mail addresses.

---

[3] Following the initial presentation of the project on 15 May 2013, a demonstration of the envisioned process was made at the subsequent meeting of the Industry Cluster, on 15 June 2013. A dedicated section was made available on the OPCW external server to share updates with the States Parties on the project.

[4] For a report of the coverage of the SIX project during these events, see "Report of the Fourth User-Group Forum for the Electronic Declaration Tool for National Authorities (EDNA)", S/1146/2014, dated 7 January 2014, and "Status Report on the Verification Information System", EC-75/S/4, dated 15 January 2014.

15. States Parties should immediately notify the Secretariat of any changes in the names and contact details of the persons designated as authorised to receive and/or transmit information through SIX, as well as changes in access to the SIX system, such as discontinuance due to, for example, changes in job responsibilities or termination of employment, in order to avoid any unauthorised disclosure of information transmitted through SIX. States Parties are also requested to nominate one of the designated persons as a primary contact point for the use of SIX.

16. For each of the designated persons, States Parties are requested to provide the fingerprint of the public portion of the cryptographic key pair[5] that will be used for protection of the information to be exchanged between the designated persons and the Secretariat through SIX. Further information about the ways in which cryptographic keys are generated and identified is available in the user manuals and guidelines posted in the dedicated section of the OPCW external server.[6]

17. In addition, States Parties are requested to specify the maximum level of information classification that the Government of that State Party accepts for receipt through SIX. Some States Parties may choose to receive information at all classification levels through the system, namely, OPCW Highly Protected, OPCW Protected, OPCW Restricted, or Unclassified, while others may choose to receive only information classified at a certain level or levels or only unclassified information. This is a matter of discretion for each State Party. In the absence of an explicit specification of the level of classification, the Secretariat will seek to clarify this with the State Party but, until such clarification is obtained, will assume that only unclassified information is authorised to be transmitted through SIX.

18. To facilitate communication of the required information, those States Parties interested in using the SIX system are requested to complete the registration form contained in Annex 2 to this Note and to return it to the Declarations Branch of the Secretariat through the diplomatic channel.

19. Any State Party requesting access and use of SIX can at any time request the Secretariat to discontinue such access and use, and can revert to the submission of information through traditional means. The issuance of an account to access SIX does not obligate the States Party to use it as its only means to exchange information with the Secretariat. States Parties can continue submitting information through more traditional means whilst also utilising SIX.

20. The Secretariat has made the necessary documentation on registering, accessing, and using the SIX system available on the dedicated section of the OPCW external server.

---

[5] According to the encryption standard used within SIX, a cryptographic key pair consists of two keys, namely the public and the private keys. Whilst the public keys are exchanged between parties that are involved in encrypted communication, the private keys are to be safeguarded by the key owners and are not to be disclosed to other parties under any circumstances. A public key fingerprint is a short sequence of bytes used to authenticate or look up a longer public key.

[6] See the "SIX Documents" link on the left-hand side of the OPCW external server home page.

21. Any questions and/or comments concerning SIX can be sent to:

Data Analytics, Reporting and Quality Control Section
Declarations Branch, Verification Division
OPCW
Johan de Wittlaan 32
2517 JR The Hague
Netherlands

Telephone: +31 (0)70 416 3026 or +31 (0)70 416 3037
Fax: +31 (0)70 306 3535
E-mail: six@opcw.org

Annexes:

Annex 1: Terms and Conditions for the Use of SIX
Annex 2: Registration Form

Annex 1

TERMS AND CONDITIONS FOR THE USE OF THE SIX SYSTEM

1. The access to and use of the Secure Information Exchange (SIX) system are subject to the acceptance by the States Parties and their designated authorised users of the terms and conditions set forth below.

Definitions and abbreviations

2. For the purpose of these terms and conditions:

"Convention" means the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, also referred to as the Chemical Weapons Convention;

"Information" is understood as defined in the OPCW Policy on Confidentiality; in particular, information may take the form of computer-generated files encrypted for the purpose of their secure transmission;

"OPCW Policy on Confidentiality" refers to the policy contained in the Annex to the decision of the Conference of the States Parties entitled "Guidelines for Procedures on the Release of Classified Information by the OPCW, in Accordance with Subparagraph 2(c)(III) of the Confidentiality Annex; A Classification System for Levels of Sensitivity of Confidential Data and Documents, Taking into Account Relevant Work Undertaken in the Preparation of the Convention, in Accordance with Subparagraph 2(d) of the Confidentiality Annex; Recommendations for Procedures to Be Followed in Case of Breaches or Alleged Breaches of Confidentiality, in Accordance with Paragraph 18 of the Confidentiality Annex (Paris Resolution, Subparagraphs 12(u), (v), and (w))" (C-I/DEC.13/Rev.1, dated 2 February 2006);

"Party" or "parties", when referred to collectively, means either the SIX user or the OPCW Technical Secretariat (hereinafter "the Secretariat") or both of them, as the case may be;

"SIX" means secure information exchange;

"State Party" means a State Party to the Convention; and

"User" means: (1) the Government of a State Party that has officially notified the Secretariat of its acceptance to receive from, and/or transmit to, information through SIX by submitting the designated registration form to the Secretariat; and (2) a person designated by the Government of a State Party as authorised to receive from, and/or transmit to, the Secretariat information through SIX and whose name, job title, telephone number, and e-mail address, as well as the fingerprint of the public portion of the cryptographic key pair that will be used for protection of the information to be exchanged between the designated person and the Secretariat through SIX, have been officially communicated by that Government to the Secretariat.

Authentication of the users and unauthorised access to or use of SIX

3. The access to and use of the SIX system are restricted to the individuals whose names, job titles, telephone numbers, e-mail addresses, and the fingerprints of the public keys have been officially communicated to the Secretariat as a representative of a State Party authorised to receive and/or transmit information through SIX on behalf of that State Party. Unauthorised access to or use of the SIX system is strictly prohibited.

4. The user of the SIX system is responsible for securing the authentication information, such as user name, e-mail address, passwords, and private key, from unauthorised access.

5. By accessing or using the SIX system, the user automatically agrees to the terms and conditions set forth herein, logging of all actions performed on the SIX system, and system monitoring for network administration and security purposes. Furthermore, the user accepts that logged actions can be used in case of investigations or disputes.

6. The Secretariat reserves the right to suspend or disable the user account if unauthorised or suspicious activities are observed during the routine monitoring of SIX by the Secretariat.

7. Individuals accessing or using the SIX system without authority or in excess of the granted authority are advised that relevant information relating to possible abuse or criminal conduct may be provided by the OPCW to appropriate state authorities in order to trigger administrative or civil action or criminal prosecution, which may result in severe penalties, including civil monetary or criminal penalties.

Authorised transmission of information through SIX

8. While SIX allows the transmission of any information encrypted according to the standards and guidelines specified by the Secretariat, irrespective of the type of the original file containing it, its format, and its classification level, the user is advised that only declarations pursuant to Articles III and VI of the Convention and relevant parts of the Verification Annex, and related documentation should be transmitted through SIX. Documents in any of the OPCW official languages may be transmitted through SIX.

9. For the information transmitted to the Secretariat, the user is responsible for determining the level of classification that is applicable to the information that is to be transmitted using SIX. The Secretariat is responsible for transmitting confidential information to the user according to the levels of classification authorised by the State Party on the registration form.

10. The user may provide documents requiring signatures (such as notes verbales or letters) as scanned images of the signed documents.

11. The user shall not use SIX for the transmission of information not related to the implementation of the Convention.

12. The user shall use SIX in a manner consistent with the OPCW confidentiality regime as established in the Confidentiality Annex to the Convention and the OPCW Policy on Confidentiality.

Procedure for transmission of information through SIX

13. The user is strongly advised to follow the guidelines and step-by-step procedures that are made available in the dedicated section of the OPCW external server. These documents will be updated as necessary.

14. The user is advised that there is no requirement to supplement a transmission through SIX with submission of the original signed paper version of the document(s) thus transmitted unless there is a national requirement to do so.

15. The SIX system will generate the following notifications:

(a) There will be an automatic on-screen notification to the user confirming the successful upload of the information.

(b) An automatic e-mail notification will be sent to the recipient confirming the availability of the information for download.[1]

(c) An automatic e-mail notification will be sent to the user confirming the successful download of the information by the recipient.

(d) For information transmitted to the Secretariat, a manual e-mail confirmation will be sent to the user, with a copy to the Permanent Representative, confirming the successful processing of the information transmitted.

16. While using SIX for the transmission of certain information, the user may continue submitting other information to the Secretariat through more traditional means (in hard copy or on CD-ROM).

Correction of information transmitted through SIX

17. In the event that the user transmits incomplete content to the Secretariat, the user is required to either amend the information or retransmit it in full, clearly specifying the purpose of the retransmission in relation to the original information transmitted.

18. In the case of technical problems with receipt by the Secretariat of information transmitted through SIX, the Secretariat will contact the user to request retransmission of the information after following the guidelines to mitigate the issue. Similarly, if the user is unable to receive the information transmitted by the Secretariat due to technical problems, the user should contact the Secretariat and request retransmission of the information.

---

[1] In addition, the user can request at the time of the transmission that a copy of the notification be sent to his/her registered e-mail address.

19. In the event of an unintended or inappropriate transmission of information by the user through SIX, the user can recall the transmission, in which case the Secretariat should be notified as to the reason for this recall.

20. In the event of an unintended or inappropriate transmission by the Secretariat of information through SIX, for example, information classified at a level for which the State Party has not authorised the use of SIX as a means of transmission, the Secretariat will recall the transmission and notify the user as to the reason for this recall. The Secretariat will develop appropriate procedures to minimise such occurrences and use the existing confidentiality framework to respond to any possible unintended or inappropriate transmission.

Date and time of information transmitted through SIX

21. Any information, including that with a specific deadline, transmitted by the State Party to the Secretariat through SIX is deemed to have been submitted on the date and time of the successful upload by the user of the file(s) to be transmitted, as indicated in the notification confirming such upload received by the user. The verification of the submission date is subject to the successful downloading. Dispatch shall be deemed unsuccessful if the user does not receive a notification confirming the successful download. In case of unsuccessful dispatch due to technical problems within the SIX system, the State Party on behalf of which the user unsuccessfully transmitted information through SIX shall not be held in breach of its obligations to submit such information within the time frame specified by the Convention.

22. Any information transmitted by the Secretariat to the State Party through SIX is deemed to have been received by the State Party on the date and time of the first successful download by the user of the submitted file(s), as indicated in the notification confirming such download received by the Secretariat. Dispatch shall be deemed unsuccessful if the Secretariat does not receive a notification confirming the successful download. In case of unsuccessful dispatch due to technical problems within the SIX system, the Secretariat shall not be held in breach of its obligations to submit such information within the time frame specified by the Convention.

Protection of the information transmitted through SIX

23. Any party shall be responsible for the protection of the information transmitted through SIX, consistent with the Convention, in particular its Confidentiality Annex, and the OPCW Policy on Confidentiality, and may be held liable in case of unauthorised disclosure of such information. Protection of information includes but is not limited to a proper digital signature and encryption of the information intended for transmission through SIX.

24. Upon receipt of information through SIX, the user shall treat that information in accordance with its level of sensitivity and with national rules and regulations. Specific handling and protective procedures shall be applied on a continuous basis in respect of such information in accordance with the Convention, in particular its Confidentiality Annex, and the OPCW Policy on Confidentiality.

25. For the information transmitted to the Secretariat by the user, the Secretariat is responsible for the protection of information from the time of the successful upload of the file(s) containing the information shown in the notification received by the user.

26. For information transmitted to the user by the Secretariat, the Secretariat is responsible for the protection of information until the time of the first download of the file(s) containing the information shown in the notification received by the Secretariat.

27. The State Party shall report as soon as possible to the Office of Confidentiality and Security of the Secretariat any potential security incidents that may be related to the use of SIX. The Secretariat will investigate such incidents according to established procedures and will report the outcome of the investigation to relevant parties.

Handling and management of cryptographic keys

28. Key generation: Cryptographic keys are used for protection of information that is to be transmitted using SIX. The States Parties are responsible for generating cryptographic keys that will be used by the designated users, following the guidelines available in the dedicated section of the OPCW external server. When generating cryptographic keys, the States Parties shall comply with the recommendations and minimum security requirements as specified in the user guidelines available on the OPCW external server.

29. Key exchange: The public portion of the cryptographic key pair of the authorised users shall be provided to the Secretariat through the diplomatic channel along with the completed registration form. The State Parties shall download the public portion of the cryptographic key pair of the Secretariat from the OPCW external server and import it into their systems, following the relevant guidelines to complete the set-up.

30. Protection of cryptographic keys: The Secretariat is responsible for protecting the private portion of its cryptographic key pair. The user or the designated person of the State Party is responsible for protecting the private portion of the user's cryptographic key pair. At the time of initial set-up and, thereafter, when the cryptographic keys are renewed, the user and the Secretariat are responsible for verifying the integrity and authenticity of the public portions of the cryptographic key pairs.

31. Key revocation: If the cryptographic key of a user is not accessible or has been compromised, the State Party shall inform the Declarations Branch of the Secretariat, in writing and as soon as possible, that the cryptographic key is no longer valid. The Secretariat may initiate a security investigation in order to assess a potential breach of confidentiality.

32. Key expiration: If the cryptographic key is about to expire or has expired, the State Party shall generate the new cryptographic key and provide its public portion to the Secretariat through the diplomatic channel in replacement of the expired key. In such cases, until this information is provided to the Secretariat, the Secretariat will not transmit any information via SIX to the respective user.

33. Withdrawal of keys: If a State Party wishes to remove the authorisation previously given to an individual identified to the Secretariat as an authorised user of the SIX system, the State Party shall notify the Secretariat through the diplomatic channel that the key has been withdrawn. The Secretariat will remove the key from the key management system.

Limitations, alteration, change, or discontinuation of the availability and services of SIX

34. The SIX system is provided by the Secretariat as a courtesy to States Parties. The Secretariat retains its exclusive right, at its sole discretion, to alter, limit, or discontinue the availability of the SIX system at any time.

35. The SIX system contains third-party applications that are not fully under the control of the Secretariat. While the Secretariat has concluded appropriate contractual agreements to safeguard the interests of the Secretariat to the maximum practical extent, ultimately the Secretariat is not responsible for discontinuation, service changes, limitations, or malfunction inherent in or associated with these third-party applications or other risks associated with the electronic transmission of information.

36. The arrangements provided under these terms and conditions are to ensure the security of the system; thus, the Secretariat cannot be responsible in case of breach of the terms and conditions by the user or any other person.

Modification of the terms and conditions

37. The Secretariat may modify the present terms and conditions at any time. The States Parties will be notified of the modifications by way of notices posted on the dedicated section of the OPCW external server and by notification through SIX. Modifications shall become effective upon the date of the posting of the modified terms and conditions. Continued access to or use of the SIX system by the user is deemed to be acceptance of the modified terms and conditions.

License restrictions

38. The SIX system contains licensed materials of third parties, the use of which is granted to the Secretariat with certain limitations and restrictions. The licence granted to the Secretariat is limited to the use of the components of SIX by the designated authorised users.

39. The user shall not reverse engineer, decompile, disassemble or otherwise attempt to derive the source code, data structures, interfaces, techniques, processes, algorithms, expertise, or other information from the components of the SIX system or permit or induce any other person to attempt the same.

40. The user shall not copy the components of the SIX system without prior authorisation from the Secretariat.

41. The user shall not transfer, sell, license, sublicense, outsource, rent, or lease the components of the SIX system or make them otherwise available for third-party use.

Liability

42. The user shall indemnify, defend, and hold harmless the OPCW, the Secretariat, and its personnel from and against any suits, proceedings, claims, demands, losses, and liability of any nature or kind, brought by any third party, based on, arising from, or relating to any acts or omissions of the user in the implementation of these terms and conditions.

43. Where the access to or use of the SIX system requires the procurement and/or installation of software or hardware components, the user shall retain sole responsibility and liability in respect of such procurement and/or installation operations.

Privileges and immunities

44. Nothing herein shall constitute or be considered to be a limitation upon or a waiver of the privileges and immunities accorded to the OPCW under the Convention, pursuant to agreements concluded with States Parties, or that it otherwise enjoys, which are specifically reserved.

Dispute settlement

45. Unless the dispute relates to a breach or an alleged breach of confidentiality, in which case the dispute shall be settled in accordance with the procedure set forth in Part IX of the OPCW Policy on Confidentiality, the parties shall use their best efforts to amicably settle any dispute, controversy, or claim arising out of, or in connection with, the use of SIX. Where the parties wish to seek such an amicable settlement through conciliation, the conciliation shall take place in accordance with the Conciliation Rules of the United Nations Commission on International Trade Law (UNCITRAL) pertaining at the time the conciliation is initiated, or according to such other procedure as may be agreed between the parties in writing.

46. Any dispute, controversy, or claim between the parties arising out of the use of SIX, unless settled under paragraph 45 above, shall, within sixty (60) days after receipt by one party of the other party's written request for such amicable settlement, be referred by either party to arbitration in accordance with the UNCITRAL Arbitration Rules pertaining at the time the arbitration is initiated. The decision of the arbitral tribunal shall be based on general principles of international commercial law. The arbitral tribunal shall have no authority to award punitive damages. In addition, the arbitral tribunal shall have no authority to award interest in excess of the London Inter-Bank Offered Rate (LIBOR) prevailing at the time the decision of the arbitral tribunal is issued, and any such interest shall be simple interest only. The parties shall be bound by any arbitration award rendered as a result of such arbitration as the final adjudication of any such dispute, controversy, or claim.

Annex 2

REGISTRATION FORM

(FOR NOTIFYING THE TECHNICAL SECRETARIAT OF THE STATE PARTY REPRESENTATIVES AUTHORISED TO EXCHANGE INFORMATION THROUGH SIX AND OF THE APPROPRIATE CLASSIFICATION LEVEL OF INFORMATION AUTHORISED TO BE TRANSMITTED THROUGH SIX)

_____ (State Party) accepts the use of the Secure Information Exchange (SIX) system and agrees to the terms and conditions governing its use (as set forth in Annex 1 of the Note by the Technical Secretariat, S/1192/2014, dated 1 July 2014) for the purpose of: ☐ Transmitting information to the Technical Secretariat ☐ Receiving information from the Technical Secretariat If this form is a modification of an existing account, please indicate whether it is an addition to or a replacement of a previously submitted notification: ☐ Addition: Previously designated users and establishments are still authorised. ☐ Complete replacement: Cancel access rights of previously designated users. ☐ Partial replacement: Access rights of the users listed below are to be cancelled. Users to be replaced:
The following persons are hereby designated by the State Party as authorised to receive from, and/or transmit to, the Technical Secretariat information through SIX:
Primary contact:
Name:
Job title:
E-mail address:
Telephone number:
Public key fingerprint:
Secondary contact:
Name:
Job title:
E-mail address:
Telephone number:
Public key fingerprint:

The State Party, having agreed to receive information from the Technical Secretariat using SIX, authorises the Technical Secretariat to transmit information according to the level of classification indicated below:

☐ Authorisation for Unclassified information

☐ Authorisation for OPCW Restricted information

☐ Authorisation for OPCW Protected information

☐ Authorisation for OPCW Highly Protected information

The State Party, having accepted the terms and conditions governing the use of SIX, undertakes to ensure that the above-designated authorised SIX users comply with such terms and conditions.

_____

Signature of the Head of the National Authority

- - - o - - -