OPCW Technical Secretariat

S/2404/2025
16 May 2025
Original: ENGLISH

NOTE BY THE TECHNICAL SECRETARIAT

UPDATE ON THE SECURE INFORMATION EXCHANGE SYSTEM

INTRODUCTION

1. The timely exchange of information between the States Parties and the Technical Secretariat (the Secretariat) is crucial for the effective and efficient implementation of the provisions of the Chemical Weapons Convention (the Convention).

2. The traditional way of exchanging classified information, through diplomatic pouch, imposes logistical difficulties. These can cause delays and may, therefore, adversely affect the timely fulfilment by the States Parties of their obligations under the Convention, including the timely submission of declarations. This may also have repercussions for important activities carried out by the Secretariat, such as the evaluation of declarations and the planning of inspections.

3. To address this issue, the Secretariat has designed and put in place a system for the secure electronic transmission of classified and unclassified documents, known as the Secure Information Exchange System (SIX), in accordance with the Note by the Secretariat on this subject (S/1192/2014, dated 1 July 2014).

4. Following detailed consultations with States Parties in the form of online discussions, and in order to further extend the use of SIX, the Secretariat has amended the terms and conditions for the use of the system as well as the SIX registration management form (Annexes 1 and 2 hereto). Accordingly, the updated terms and conditions and registration management form supersede those published in Annexes 1 and 2 to Note S/1192/2014, as well as any updates thereto.

5. This Note describes the amended terms and conditions and use of SIX, the current status of the system, as well as the future priorities for this critical communication mechanism. A previous update was provided to the States Parties last year (S/2291/2024, dated 27 May 2024).

AMENDED TERMS AND CONDITIONS AND USE OF THE SECURE INFORMATION EXCHANGE SYSTEM

6. The amended terms and conditions broaden the types of classified information that can be disseminated to the States Parties through SIX, while ensuring that the provisions of the OPCW Confidentiality Regime continue to be met. The amended terms and conditions simplify the registration process and make SIX available to more users. The

amended terms and conditions (Annex 1), together with the amended registration management form for the use of SIX (Annex 2) allow SIX users to:

(a) receive documents from the Secretariat through SIX, up to the highest OPCW classification level ("OPCW Highly Protected");

(b) send documents to the Secretariat through SIX at any level of classification; and

(c) receive classified documents containing States Parties' information, including from States Parties that are not registered SIX users.

7. The above arrangements expand the update on the use of SIX as previously described in Secretariat Note S/1525/2017/Rev.1 (dated 19 September 2017). Examples of documents that may be transmitted through SIX include, but are not limited to, transfer discrepancy notes verbales, biannually distributed redacted declarations, and the annual Verification Implementation Report. Documents will be transmitted by the Secretariat through SIX only to registered users.

8. In addition, the amended SIX terms and conditions are applicable to both the (registered) States Parties as well as (registered) designated laboratories.

9. 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 established handover arrangements while ensuring compliance with the OPCW Confidentiality Regime.

10. The use of SIX is subject to the acceptance by States Parties or designated laboratories of the terms and conditions set forth in Annex 1 to this Note, after registration using the form contained in Annex 2 and 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 or designated laboratories will be required to accept the terms and conditions, which will be referenced on the SIX portal home page.

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

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

13. For each of the designated persons, States Parties or designated laboratories are requested to provide the fingerprint of the public portion of the cryptographic key pair[1] that will be used to protect 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 Catalyst platform.[2]

14. To facilitate communication of the required information, those States Parties or designated laboratories interested in using SIX 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 via email (six@opcw.org).

15. Please note that the designated person(s) who are already registered at the date of this Note are not required to resubmit the registration management form.

16. Any State Party or designated laboratory requesting access to 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 established handover arrangements while ensuring compliance with the OPCW Confidentiality Regime. The issuance of an account to access SIX does not obligate the State Party to use it as its only means to exchange information with the Secretariat.

17. The Secretariat has made the necessary documentation on registering, accessing, and using SIX available on the dedicated section of the Catalyst platform.[2]

OVERVIEW OF SYSTEM USE

18. SIX is an established system for secure communication between the Secretariat and the States Parties. As at 30 April 2025, 67 States Parties had registered for SIX, resulting in the authorisation of 124 active users to use the system.

19. States Parties from all OPCW regional groups are represented among the users of SIX, with 32.2% of users from the Group of Western European and Other States, 26.6% from Asia, 21.8% from Latin America and the Caribbean, 15.4% from Eastern Europe, and 4.0% from Africa.

20. As at 30 April 2025, 40 annual declarations on past activities (ADPAs) for 2024 had been submitted using SIX, which represents 51.9% of the total number of declarations received by the Secretariat (77 ADPAs for 2024 as at 30 April 2025). The use of electronic declaration transmission enables States Parties to dedicate more time to the preparation of declarations and to benefit from a more efficient and streamlined declaration submission process.

---

1 According to the encryption standard used within SIX, a cryptographic key pair consists of two keys, namely, the public and private keys. While 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.

2 See the "SIX downloads" link on the SIX Catalyst site available at: https://catalyst.opcw.org/sites/VRT/sitepages/six.aspx.

21. Since the initial release of SIX in 2014, the Secretariat has received 2,338 documents from States Parties through the system. The majority of these documents have been annual declarations on past and anticipated activities, as well as amendments to previously submitted declarations under Article VI of the Convention. In addition, other types of documents have been received via SIX, including declarations under other articles of the Convention, responses to official letters from the Secretariat, and operational documents related to SIX itself. A total of 14.8% of all documents received via SIX are unclassified.

CURRENT AND FUTURE ACTIVITIES

22. Since SIX was launched, the Secretariat has continued to provide support to the States Parties with regard to registering and using the system, enhancing the system's security and usability, and promoting the benefits of its use. Presentations and demonstrations of SIX have been included in training courses provided by the Secretariat for National Authorities.

23. The Secretariat is preparing an information graphic to illustrate SIX procedures, accompanied by responses to frequently asked questions, for publication on the Catalyst platform in the latter half of 2025.

24. In order to ensure that SIX is available to users and remains a secure means of transmission, the Secretariat carries out regular system updates, maintenance, and security audits.

CONCLUSION

25. Since its initial launch, SIX has continued to create efficiencies for the Secretariat and the States Parties by providing a secure mechanism to transmit classified information. The Secretariat encourages States Parties and designated laboratories to consider registering for SIX in order to avail themselves of the benefits the system provides.

26. Further administrative and technical questions concerning SIX can be sent to:

Data Analytics, Reporting and Quality Control Section (DARQ)
Declarations Branch, Verification Division
OPCW
Email: six@opcw.org

Any other requests may be sent by email to:

Declarations Branch, Verification Division
OPCW
Email: deb@opcw.org

Annexes:

Annex 1: Terms and Conditions for the Use of the Secure Information Exchange System

Annex 2: Secure Information Exchange System Registration Management Form

Annex 1

TERMS AND CONDITIONS FOR THE USE OF THE SECURE INFORMATION EXCHANGE SYSTEM

1. This document establishes the terms and conditions for the use of the Secure Information Exchange System (SIX), which supersede the terms and conditions published in Annex 1 to Note S/1192/2014 (dated 1 July 2014) by the Technical Secretariat (the Secretariat) and any updates thereto.[3]

2. SIX is maintained by the Secretariat. Access to and use of the system are subject to the acceptance by users, including States Parties, designated laboratories, and their designated and authorised users, of the terms and conditions set forth below.

Definitions and abbreviations

3. For the purpose of these terms and conditions:

"Catalyst" means the dedicated part of the OPCW external server whereby the verification-related tools may be accessed by the States Parties online (https://www.opcw.org/resources/catalyst/register);

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

"Designated laboratory" means a laboratory accredited by the OPCW for the off-site analysis of environmental or biomedical samples at the request of the Secretariat, provided there is a technical arrangement in place between the OPCW and the designated laboratory;

"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 Confidentiality Regime" means the rights, obligations, policies, procedures, and/or principles contained in the Confidentiality Annex to the Convention; the OPCW Policy on Confidentiality (C-I/DEC.13/Rev.2, dated 30 November 2017), and any subsequent amendments thereto; the OPCW Manual of Confidentiality Procedure, and other related documents;

"Party" or "Parties" means either the SIX user or the Secretariat, or both collectively as the case may be;

"SIX" means the Secure Information Exchange System first described in Note by the Secretariat S/1192/2014 and further updated in Note S/2404/2025 (dated 16 May 2025);

---

[3] The technical and operational aspects of SIX are provided in annual updates by the Secretariat. The latest such update as at the date of these terms and conditions is contained in Note S/2404/2025 (dated 16 May 2025).

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

"Technical arrangement" means an agreement/arrangement between a designated laboratory and the OPCW. These pertain, inter alia, to the off-site analysis of samples at the request of the Secretariat;

"User" means: (1) the Government of a State Party or a designated laboratory that has officially notified the Secretariat of its acceptance to receive from and transmit to the Secretariat information through SIX, by submitting the registration management form to the Secretariat; and (2) a person designated by the Government of a State Party or designated laboratory as authorised to receive from, and transmit to the Secretariat information through SIX, and whose name, job title, email address, telephone number, user type (namely, National Authority, designated laboratory, or Other), token delivery mode, and 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 or designated laboratory to the Secretariat. Four users may be designated by the State Party and two by a designated laboratory;

"Guidelines" means the user guidelines as defined and available on the dedicated section of the Catalyst platform (https://catalyst.opcw.org/sites/VRT/sitepages/six.aspx).

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

4. The access to and use of SIX are restricted to users, as defined above. Unauthorised access to or use of SIX is strictly prohibited.

5. The user of SIX is responsible for securing from unauthorised access the authentication information, such as username, email address, passwords, multifactor authentication codes, and private key.

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

7. 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.

8. Individuals accessing or using SIX 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.

9. States Parties and designated laboratories are responsible for notifying the Secretariat of changes to their registered users by using the registration management form attached as Annex 2 to S/2404/2025 (dated 16 May 2025). The form should be used for new registrations as well as for deregistration of existing users.

Authorised transmission of information through SIX

10. 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 agrees that only verification-related information, including declarations pursuant to Articles III and VI of the Convention and relevant parts of the Verification Annex to the Convention, shall be transmitted through SIX.

11. Documents in any of the OPCW official languages may be transmitted through SIX.

12. The user is responsible for determining the level of classification that is applicable to the information that is transmitted by the user to the Secretariat through SIX.

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

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

15. The user shall use SIX in a manner consistent with the Convention and the OPCW Confidentiality Regime.

16. The Secretariat may transmit information to the SIX users up to the classification of "OPCW Highly Protected". The encrypted files transmitted through SIX may contain classified information submitted to the Secretariat by or related to any State Party to the Convention. Examples of documents that may be transmitted through SIX include, but are not limited to, declarations, inspection reports, transfer discrepancy notes verbales, biannually distributed redacted declarations (informally referred to as a "batch"), and the annual Verification Implementation Report. Documents will be transmitted by the Secretariat through SIX only to registered users.

Procedure for transmission of information through SIX

17. The user shall follow the guidelines and step-by-step procedures that are made available on Catalyst. These documents will be updated as necessary.

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

19. SIX will generate the following notifications:

    (a) an automatically generated on-screen notification to the user confirming the successful upload of the information; [4]

    (b) an automatically generated email notification to the recipient confirming the availability of the information for download;

[4] In addition, the user can request at the time of the transmission that a copy of the notification be sent to their registered email address.

(c) an automatically generated email notification to the user confirming the successful download of the information by the recipient; and

(d) for information transmitted to the Secretariat by the user, an email confirmation prepared manually and sent to the user by the Secretariat confirming the successful decryption of the information transmitted. In case the user is a Government of a State Party or their designee, a copy of the email confirmation will also be sent to the Permanent Representative.

20. While using SIX for the transmission of certain information, the user may continue to submit other information to the Secretariat through established handover arrangements, while ensuring compliance with the OPCW Confidentiality Regime.

Correction of information transmitted through SIX

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

22. 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.

23. 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.

24. The Secretariat may recall a transmission and notify the user as to the reason for this recall. The Secretariat follows procedures aimed at minimising such occurrences.

Date and time of information transmitted through SIX

25. Any information transmitted by the user to the Secretariat through SIX is deemed to have been received by the Secretariat on the date and time of the first successful transmission.

26. Any information transmitted by the Secretariat to the user through SIX is deemed to have been received by the user on the date and time of the first successful transmission.

Protection of the information transmitted through SIX

27. Each party shall be responsible for the protection of the information transmitted through SIX, in compliance with the Convention and the OPCW Confidentiality Regime, 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 all information intended for transmission through SIX pursuant to the standards and guidelines specified by the Secretariat, regardless of its classification, except when sending an updated SIX public key. Information provided in the SIX email is not encrypted and therefore the email should not include classified information.

28. Upon receipt of information through SIX, the user shall treat that information in accordance with its classification and level of sensitivity and with any appropriate 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 and the OPCW Confidentiality Regime.

29. The Secretariat is responsible for the protection of information transmitted to it by the user from the time of the successful upload of the file(s) by the user.

30. The Secretariat is responsible for the protection of information transmitted by it to the user until the time of the first successful download of the file(s) by the user.

31. The user 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 on the outcome of the investigation to relevant parties.

Handling and management of cryptographic keys

32. **Key generation**: Cryptographic keys are used for the protection of information that is to be transmitted using SIX. The States Parties or designated laboratories are responsible for generating cryptographic keys that will be used by the designated users, following the guidelines available on Catalyst. When generating cryptographic keys, the States Parties or designated laboratories shall comply with the recommendations and minimum security requirements as specified in the guidelines.

33. **Key exchange**: The public portion of the cryptographic key pair of the authorised users shall be provided to the Secretariat through email or diplomatic channels, or using communication methods specified in a technical arrangement with the Secretariat, as the case may be, along with the completed registration management form. The States Parties or designated laboratories shall download the public portion of the cryptographic key pair of the Secretariat from Catalyst and import it into their systems, following the relevant guidelines to complete the set-up.

34. **Protection of cryptographic keys**: The Secretariat is responsible for protecting the private portion of its cryptographic key pair. The user is responsible for protecting the private portion of their 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.

35. **Key revocation**: If the cryptographic key of a user is not accessible or has been compromised, the State Party or designated laboratory 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.

36. **Key expiration**: If the cryptographic key is about to expire or has expired, the State Party or designated laboratory shall generate a new cryptographic key and provide its public portion to the Secretariat through email or diplomatic channels, or through communication methods specified in a technical arrangement with the Secretariat, as

the case may be, in replacement of the expired key. In such cases, until this information is provided to the Secretariat, the Secretariat will not transmit any information through SIX to the respective user.

37. **Withdrawal of keys**: If a State Party or designated laboratory wishes to revoke the authorisation previously given to an individual identified to the Secretariat as an authorised user of SIX, the State Party or designated laboratory shall notify the Secretariat that the key has been withdrawn, by submitting the registration management form through email, diplomatic channels, or through communication methods specified in a technical arrangement with the Secretariat, as the case may be. The Secretariat will remove the key from the key management system.

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

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

39. SIX 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 OPCW 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 electronic transmission of information.

40. The purpose of the arrangements provided under these terms and conditions and other applicable procedures is to ensure the security of the system. The Secretariat cannot be held responsible or liable in case of breach of the terms and conditions or other applicable procedures by the user or any other person or entity.

Modification of the terms and conditions

41. The Secretariat may modify the present terms and conditions at any time. The States Parties or designated laboratories will be notified of modifications by way of notices posted on Catalyst and by notification through SIX. Modifications shall become effective either upon the date of the notification of the modified terms and conditions or on the date specified in such notification for the entry into effect of the modifications, as the case may be. Continued access to or use of SIX by the user is deemed to constitute acceptance of the modified terms and conditions.

Licence restrictions

42. SIX 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.

43. 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 SIX or permit or induce any other person to attempt the same.

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

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

Liability

46. The OPCW shall not under any circumstances or for any reason whatsoever be held liable for loss, damage or injury sustained by any State Party or designated laboratory or their designated, authorised users arising from or attributable to the use of SIX. The OPCW shall not accept from any State Party or designated laboratory or their designated, authorised users any claim for compensation or repairs in respect of any such loss, damage or injury.

47. 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.

48. Where the access to or use of SIX 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

49. 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.

Dispute settlement

50. 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, as appropriate, 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. Without prejudice to the privileges and immunities of the OPCW, 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) then in effect, or according to such other procedure as may be agreed between the parties in writing.

51. Any dispute, controversy, or claim between the parties arising out of the use of SIX, unless settled as above, shall, within 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 then in effect. The number of arbitrators shall be one. The place of arbitration shall be the Permanent Court of Arbitration at The Hague, the Netherlands. The language of the arbitration shall be English. The decisions of the arbitrator shall be based on general principles of international commercial law. The arbitrator shall have no authority to award punitive

damages. In addition, the arbitrator shall have no authority to award interest in excess of the United States Federal Reserve Bank of New York's Secured Overnight Financing Rate prevailing at the time the decision of the arbitrator 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

**SECURE INFORMATION EXCHANGE SYSTEM
REGISTRATION MANAGEMENT FORM[5]**

(FOR NOTIFYING THE TECHNICAL SECRETARIAT OF THE STATE PARTY OR DESIGNATED LABORATORY USER(S) AUTHORISED TO EXCHANGE INFORMATION THROUGH THE SECURE INFORMATION EXCHANGE SYSTEM)

(State Party/designated laboratory)_____
accepts the Secure Information Exchange System (SIX) and agrees to the terms and conditions governing its use (as set forth in Annex 1 to Note by the Technical Secretariat S/2404/2025 (dated 16 May 2025), for the purpose of transmitting and receiving information up to a classification of "OPCW Highly Protected" to and 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**: Register new user. Previously registered users and establishments, if any, are still authorised.

☐ **Complete replacement:** Deregister and cancel access rights of all previously registered users.

☐ **Partial replacement:** Deregister and cancel access rights of the users listed below.

Users to be deregistered:

_____
(Email address)

_____
(Email address)

5 This form supersedes the form contained in Annex 2 to the Note by the Secretariat S/1192/2014 (dated 1 July 2014).

The following person(s) are hereby designated by the State Party/designated laboratory as authorised to receive from and transmit to the Technical Secretariat information through SIX (Note: a maximum of four users may be designated by the State Party and two by the designated laboratory):
Primary contact:
Name:
Job title:
Email address:
Telephone number:
User type: ☐ National Authority ☐ Designated laboratory ☐ Other
Public key fingerprint:
Token delivery mode: ☐ Email ☐ iPhone ☐ Android

Secondary contacts:
Name:
Job title:
Email address:
Telephone number:
User type: ☐ National Authority ☐ Designated laboratory ☐ Other
Public key fingerprint:
Token delivery mode: ☐ Email ☐ iPhone ☐ Android
Name:
Job title:
Email address:
Telephone number:
User type: ☐ National Authority ☐ Designated laboratory ☐ Other
Public key fingerprint:
Token delivery mode: ☐ Email ☐ iPhone ☐ Android
Name:
Job title:
Email address:
Telephone number:
User type: ☐ National Authority ☐ Designated laboratory ☐ Other
Public key fingerprint:
Token delivery mode: ☐ Email ☐ iPhone ☐ Android

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

_____

Name
(Head of National Authority or authorised representative of designated laboratory)

_____

Signature

_____

Date

- - - o - - -