JIU/ML/2021/1

United Nations

Management letter on securing the integrity of documents, records and archives of the United Nations system organizations

Prepared by Jorge Flores Callejas and Nikolay Lozinskiy

JIU/ML/2021/1

United Nations

Management letter on securing the integrity of documents, records and archives of the United Nations system organizations

Prepared by Jorge Flores Callejas and Nikolay Lozinskiy

INTRODUCTION

1. The Joint Inspection Unit (JIU) included a report entitled *Cybersecurity in the United Nations system organizations: a review of policies and practices* as part of its 2020 Programme of Work in line with the objectives of the Strategic Framework of the Unit. The review is expected to provide insights for participating organizations to strengthen governance, enhance accountability, identify priority areas to improve overall cyber-resilience and to lower exposure to cyber-risks. During the preparation of the report, the Inspectors were informed of risks associated specifically with the safeguarding and protection of organizations' legal, normative, administrative, political and historical documents and data. The Inspectors believe it prudent to bring this matter in the form of a Management Letter to the attention of the executive heads of all participating organizations, for action as appropriate.

SECURING THE INTEGRITY OF DOCUMENTS, RECORDS AND ARCHIVES OF THE UNITED NATIONS SYSTEM ORGANIZATIONS

2. The members of United Nations system organizations have vested in them a custodial role with respect to intergovernmental documents, which are often the product of protracted negotiation and sensitive diplomatic processes. These documents include, but are not limited to, treaties and conventions, parliamentary documents, information given into the organizations' custody by their members, and digital and analogue information generated by the organizations themselves in fulfilling their respective mandates. If their content or any aspect of their articulation, including associated voting records, accompanying notes, chronological information, lists of participants, names or the functional capacities of persons reflected as participating in the documents' creation, were altered, particularly retroactively and without being detected for extended periods of time, it could cause considerable damage to the point of endangering international safety and security. Records related to international, diplomatic, energy, and security affairs constitute a vital category of information requiring special protection, especially in the digital ecosystem of these organisations. Similar considerations apply to administrative, operational and personal data. Administrative records form the backbone ensuring the functioning of the respective organization and its ability to carry out its mandated activities. Operational and personal data contain unique information about the work of the United Nations system organizations in the field of development and the defence of human rights. Whether such documents are stored in digital or paper form, and irrespective of whether they are archived and represent historical documentation or are in current use, possibly even subject to live debate, the protection of their integrity is undisputedly of paramount importance.

3. The "triad of information security" that encompasses the confidentiality, integrity and availability of information, including electronically stored data, highlights the essential characteristics of information that require protection, as defined with a view to focusing information holders' commitment to safeguarding all information from both external and internal interference. While availability and confidentiality aspects already enjoy high visibility and prominence, the authenticity, reliability and integrity of data, documentation and systems used to store them is less obvious and could be tampered with in dangerous and stealthy ways. Without proper integrity measures, the availability and confidentiality aspects of information security would also be put at risk.

4. A JIU report on records and archives management[1] issued in 2013 underlined the importance of protecting the physical and electronic environment where data is stored, limiting access to information or content that is considered confidential, restricted or secret and retaining and safeguarding all records considered to be of permanent value. It also highlighted inherent risks at the time in terms of integrity, security and authenticity as digital records could potentially be easily modified, deleted and moved while

[1] JIU/REP/2013/2: *Records and Archives Management in the United Nations*.

users' actions were difficult to trace appropriately. Replications were commonly performed without detection and controls to safeguard their integrity were limited. Some of these risks may continue to persist today.

5. United Nations system organizations have introduced a variety of digital systems to facilitate access to their records and archives, including to diplomatic delegations, governments, researchers and the wider public. These systems have eliminated some challenges, yet brought about others, including new risks associated with preserving the systems' own authenticity, usability and integrity. The United Nations system organizations, on different occasions, stated that their ICT systems are facing increasing risks, as they are exposed to external and internal threats which are significant and growing in scale and complexity and further exacerbated by vulnerabilities related to the lack of effective and efficient cybersecurity management and investment. These risks and challenges grow more critical as the volume of records, including those in digital format, increases. On the occasion of the preparation of the report on cybersecurity, the Inspectors received indications that this risk is not hypothetical but amounts to a real threat and confirmed that participating organizations have encountered difficulties of that kind.

6. Some effective preventive measures for preserving data and content integrity might be taken through the careful design of information systems architecture (for example using document checksums, digital signatures, change logs and similar techniques), but there is an acute need to address data integrity throughout the entire lifecycle of documents. There are emerging technological solutions with data integrity in focus, which might also be studied by organizations for use in building tampering-resistant archives.

7. It is critical for organizations in the United Nations system as custodians of documents of global importance to ensure that they are secure and their integrity is protected against risks and threats, including cyber-risks. A number of organizations have already implemented sophisticated Enterprise Content Management (ECM) systems and other measures in this regard. The Inspectors urge participating organizations that have not yet done so to increase their attention to devising and applying appropriate safeguards to secure their current and historical documents, records and archives, including by revisiting, if necessary, the security parameters applied to the storage of such documents in both the physical and cyber-environment with a view to maximally protecting them from being tampered with. The most appropriate controls to ensure not only the completeness, accuracy, consistency and reliability of information in this regard, but also its authenticity, integrity and encryption, where applicable, should be identified according to the level of protection required to match each organization's own situation based on a dedicated risk assessment focusing on the integrity aspect of cybersecurity.

Recommendation 1

The Inspectors request the executive heads of United Nations system organizations to give due consideration to devising and applying appropriate safeguards to secure their current and historical documents, records and archives including by revisiting, if necessary, the security parameters applied to the storage of such documents in both the physical and cyber-environment and including the matter in their organizations' risk registry, and to report to the Joint Inspection Unit through the web-based tracking system no later than the end of 2022 on the measures taken to implement the present recommendation.