Government Resolution No. 2443 of February 15, 2015

33rd Government of Israel – Benjamin Netanyahu

**Resolution: Advancing National Regulation and Governmental Leader
Cyber Security**

It is hereby resolved:

Further to Government Resolution No. 3611 of August 7, 2011, regarding "Advancing the National Capacity in Cyberspace" (hereinafter: Resolution 3611), and in accordance with the national policy in cyber security, in methodically and continuously increase the level of security in cyberspa State of Israel, and subject to Government Resolution No. 2282* of October 26, 2014:

To advance national regulation in cyber security, and to work for gover leadership in cyber security as part of the implementation of national regulati to serve as an example for the public and the economy.

This regulation will not apply to the defense community or to its activities thr government offices as part of its missions.

Definitions:

Cyber security services market – companies, manufacturers, suppliers, trainin certification institutions and professionals who provide know-how, produc services in cyber security to organizations.

Sector – all the organizations working as part of the professional field of government office and in the framework of its regulatory authority.

1. In the field of national regulation in cyber security:

   a. To adopt the principles from the policy of national regulation in security (hereinafter: the Policy) formulated by the National Cyber Bur

* regarding Reducing the Regulatory Burden

(hereinafter: the Bureau), which includes regulating the cyber sec services market, alongside regulating the preparedness of organizatio the economy in this field, detailed in Addendum A.

b. In accordance with the Policy, to determine that regulating the preparedness of organizations in the economy in the field of cyber secu be conducted with the intention to not add more regulators to the economy, but rather to strengthen existing regulators through a r tools at their disposal and to bolster these tools as needed in or increase the level of resilience in the civilian sector against cybe including through preparedness and training.

c. To charge the Bureau with the task of establishing a unit whose missio to regularize the cyber security services market, including profes services and products, in accordance with the Policy and subject to all as detailed in Addendum B. The unit will be established as part National Cyber Security Authority that is planned to be part of the Prin Minister's Office, subject to government resolution (hereinafter: the National Cyber Security Authority).

d. To charge the Bureau with the task of examining the building of infrastructure for inspecting and approving cybersecurity products, including examining the establishment and operation of a lab to this en detailed in Addendum C.

e. To charge the directors general of the government offices, in the framework of which regulatory authority is exercised vis-à-vis organizations or activities that are exposed to cyber threats, to a preparedness against cyber threats within the sector in which they ope as follows:

i. To establish a unit for professional guidance in the field of cy security, as detailed in Addendum D, in accordance with the regula authority they exercise.

ii. To work to determine policy and regulation requirements in order t implement this Resolution in the framework of the sector for which they are responsible.

iii. To carry out, in coordination with the Bureau, staff work to b presented to the prime minister which examines the amendments a changes required from a legal perspective to effectively realiz aforementioned.
In sectors in which more than one government office is respo for exercising regulatory authority concerning organizations or activities, to charge the Head of the Bureau to determine which off will take the lead on this activity.

f. To instruct the director general of the Ministry of Economy, in coordination with the Bureau and the Ministry of Finance, to pre the Government within 120 days of the passing of this Resolution, a pl to implement assistance and incentive mechanisms for organizations i economy that work to increase the level of preparedness against threats, as defined in the plan.

g. To charge the legal department of the Prime Minister's Office an Bureau, in cooperation with the Ministry of Justice, to prepare a memorandum to be presented by the prime minister, and to cons the legislative amendments needed to implement the aforementioned within 180 days of this Resolution being passed.

2. <u>In the field of governmental leadership in c</u>yber security:

a. To establish a unit for cyber security in the government (herein YAHAV), with the mission of serving as the body responsible for providing guidance and professional instruction in the field of cyber security for all government offices and auxiliary units, excluding the defense community, and to establish a governmental command and co center for cyber threats (hereinafter: the Governmental SOC), as deta Addendum E.

b. To charge the directors general of the government offices and the dire of the auxiliary units to act to improve the level of cyber security, and t that end to appoint a cyber security administrator, establish a st committee, regularize the professionals in the field of cybersecurity employed in the office, allocate a designated budget for cyber security part of the existing office budget and ensure that the office mee

standards of organizational information security, as detailed in Addendum F.

c. To charge the Director of Government Procurement and the direc general of government offices, where relevant, with the task of determining, as part of the central procurement process or as part of t offices' procurement process, appropriate requirements in the fiel cyber security, as detailed in Addendum G.

d. To charge the Director of the Bureau with the task of establishin steering committee for the advancement of governmental leadersh cybersecurity (hereinafter: the governmental steering committee) and formulating assistance mechanisms for government offices so that might implement advanced technological solutions for unique nee detailed in Addendum H.

e. To charge YAHAV with the task of ensuring that Articles 2(b) and 2(c) o this Resolution are implemented and reporting back to the governmen steering committee in this regard.

3. To charge the Bureau and the Ministry of Defense with the task of conduc staff work to examine if and how this Resolution will apply to the Ministry Defense and its units, with attention paid to the character of its act unique authorities and the rules of procurement according to which it ope

4. The international cybersecurity activities of the National Cyber Security Authority relevant to this Resolution will be conducted in coordination wit Ministry of Foreign Affairs and with their participation, as needed.

Addendum E – Governmental Leadership in Cyber Security – The Unit Cyber Security in the Government and the Governmental Comma Control Center for Cyber Threats

1. Mission of the Unit for Cyber Security in the Government (hereinafter: YAHAV): To provide professional guidance and instruction in the field cyber security for all government offices and auxiliary units.

2. Supervisors:

   a. YAHAV will operate under the supervision of the Director of the Nation Information Technology Unit.

   b. YAHAV will operate in accordance with the professional instruction of National Cyber Security Authority.

3. Tasks:

   a. To guide and instruct government offices and auxiliary units on aspects cyber security, including the following:

      i. Mapping of objects in need of defense

      ii. Risk management

      iii. Preparation of a cyber security plan and allocation of resourc implement it

      iv. Formulation of organizational policy, regulations and work methods

      v. Preparedness to handle incidents, including managing incidents, processes for recovery and rehabilitation

      As needed, for matters that fall under the purview of the Law for Regularizing Security in Public Bodies of 1998 (hereinafter: the law), on subjects that fall under the purview of the Protection of Privacy Law 1981, instruction will be conducted in coordination with the party

authorized by these laws. In addition, as much as possible, the instruct
will be implemented while taking into account the unique needs
characteristics of the government offices and auxiliary units.

b. To supervise the implementation of the professional requirements in
accordance with the guidance and instruction.

c. To develop processes for information sharing inside the governme
including reporting to the National CERT.

d. To initiate horizontal activity and implement it.

e. To follow up on and ensure that the requirements regarding the
governmental leadership in cyber security are being met, and to repor
the governmental steering committee, as detailed in Addendum H.

4. Human Resources and Budget:
In order to establish the unit, the National Information Technology Unit w
allocate two job positions for 2015 from its resources, and the Mini
Finance will allocate two job positions for 2015 and three for 2016 in
accordance with the agreement with the Prime Minister's Office. The
employment requirements for the unit's employees will be agreed upon by
National Information Technology Unit and the Director of Wages in
Ministry of Finance, in coordination with the Bureau and the Civil S
Commission. In addition, the Ministry of Finance will allocate a budget tot
NIS 1.5 million to the unit in 2015, NIS 2 million in 2016, NIS 0.5 million
2017 and a continuous budget of NIS 4 million beginning in 2017.

Governmental Command and Control Center for Cyber Threats:

5. To charge the Bureau and YAHAV with the task of jointly establishin
governmental command and control center for cyber threats (hereina
Governmental SOC), which will work to formulate an ongoing government
situational awareness on aspects related to cyber security and provide a
response to handling cyber incidents.

6. To establish the Governmental SOC as part of the National CERT, based on its technological and operational infrastructure while building up des capabilities for the government.

7. To instruct the government offices, including E-Government, to send repor related to cyber security to the Governmental SOC, including incidents, th vulnerabilities and malware.

8. The budget for the Governmental SOC will be agreed upon by the Bureau, National Information Technology Unit and the Ministry of Finance.

Addendum F – Governmental Leadership in Cyber Security – Acti
Advance Cyber Security in Government Offices

Definition:

"Israeli Standard ISO 27001" – The Israeli standard adopted from the interna
ISO regarding the establishment of a mechanism for administering the
organizational information security and the ongoing process of its meth
improvement.

1. Appointing a cyber security administrator in government offices:

   a. The directors general of government offices will appoint in every government office a cyber security administrator for the office. This position holder will work under the direct supervision of the dire general or on their behalf.

      i. The position of the administrator will be filled, where possible, b position holder with an existing administrative rank.

      ii. Only one administrator will be appointed in each government office order to prevent duplication.

   b. The tasks of the cyber security administrator:

      i. To formulate the office's cyber security policy in in accordance with organizational risk management process.

      ii. To design a work plan for cyber security in accordance with policy.

      iii. To analyze and assess the cyber security plan and policy in an ongo manner, adjusting for needs, threats and responses, as well as of t organizational preparedness to handle cyber incidents.

      iv. To formulate a budgetary plan for cyber security and maintain it on ongoing basis.

v. To supervise the implementation and administration of cyber secur from a broad, organizational perspective, in accordance with policy

c. This person will serve as the office's representative in the gover steering committee (if the office is represented in the steering commit as detailed in Addendum H.

d. The directors of auxiliary units in a government office will appoi coordination with the government office and YAHAV, a cyber secu administrator for the auxiliary unit or alternately by cybersecurity supervisor. If the decision is made to appoint a cyber security supervis they will work under the professional guidance of the cyber secu administrator in the government office.

2. Arranging the appointment of professionals in the field of cyber sec employed in the government and by the government:

a. The governmental steering committee will define within 120 days requirements to employ professionals in the field of cyber security in t government and by the government, in accordance with the princ determined by the Bureau, while taking into account the Report Public Committee to Define Cyber Security Professions. These requirements will be examined periodically by the governmental s committee.

b. Within 90 days of the governmental steering committee's having determined the requirements, the offices will examine how closel employees in the field of cyber security meet the requirements. mapping will be presented to the governmental steering committee.

c. The offices will appoint a cyber security officer in the IT division:

i. The officer will meet the requirements determined by the governmental steering committee as aforementioned.

ii. The officer will be under the direct supervision of the CIO and wil work in accordance with YAHAV's professional instructions wit regard to cyber security aspects.

d. Any new employee hired in the field of cyber security in the governme must meet the professional requirements outlined above.

e. The governmental steering committee will define the stages of implementation for the professional requirements, including carryi professional training and education so that, within at most five y employees working in the field of cyber security in the governme meet the professional requirements. Exceptions may be approved only the governmental steering committee.

3. Establishing an office steering committee:

a. The committee will work to improve the level of cyber security i office, including the activities detailed in this Resolution, and will supe the ongoing operational activities in the office in this regard.

b. The head of the committee: the director general of the government offi members: senior representatives of the office that have responsibilities the field of cyber security, including responsibility for technological, security and operational aspects, the director of budgets, the dire human resources, the legal advisor, a representative from YAHAV additional representatives, at the director general's discretion.

c. The committee will convene at least once every six months.

4. Allocating funds designated for cyber security as part of the existing budg government offices:

a. The directors general of government offices and directors of auxi units, as part of their existing authorities and responsibilities, will regu the annual budgetary structure of their office so that at least 8% of the budget will be directed to cyber security.

b. The director general of the government office or the director of auxiliary unit, if relevant, can under special circumstances approve a reduction of the aforementioned after presenting a detailed and reason decision to the governmental steering committee as outlined in Adden H, and only if at least 6% of the IT budget is directed to cyber security.

c. At the end of two years from the date of this Resolution, the governme steering committee will examine the need to increase the percentage o budget designated for cyber security.

5. Meeting the standards for organizational information security in gove offices and its bodies:

a. The directors general of government offices will determine within 120 of the passing of this Resolution a graduated plan for the implementati certification and qualification of an organizational information sec standard from the category Israeli Standard ISO 27001, as outlined be

i. The office headquarters and regional offices – within two years. Th governmental steering committee is authorized to extend this by an additional year.

ii. Additional office bodies – in accordance with the multi-year work pl to be formulated within two years, to be implemented within at mos five years.

b. The qualification plan will be submitted for the governmental ste committee's approval as detailed in Addendum H, within 120 days of th Resolution's passing. It will be the responsibility of the directors gener the government offices to implement the approved plan.

c. The government offices will update the governmental steering commit every year about the implementation of the plan no later than June 30 that year.

d. The Bureau will advance a competitive process for consultation service provide professional help to the government offices on an individual ba when realizing the implementation plan and will fund their activity.

The above is a translation of Government Resolution No. 2443 of Febr 15, 2015. The binding language of this Government Resolution i held by the Government Secretariat in Hebrew. The binding lang draft legislation and law memoranda mentioned in this Resolutio draft published on the record. Budgetary decisions are subject to the Budget Law.