Socialist Republic of Viet Nam
Authority of Information Security (AIS),
Ministry of Information and Communications (MIS)

PROJECT ON CAPACITY BUILDING FOR CYBER SECURITY IN VIETNAM (CAREER DEVELOPMENT PLAN)

PROJECT COMPLETION REPORT

FEBRUARY, 2022

JAPAN INTERNATIONAL COOPERATION AGENCY (JICA)

JAPAN DEVELOPMENT SERVICE CO., LTD (JDS)

GP
JR
22-034

TABLE OF CONTENTS

ANNEX

LIST OF TABLES

I. Basic Information of the Project

1. Country

Socialist Republic of Viet Nam

2. Title of the Project

Project on Capacity Building for Cyber Security in Viet Nam

3. Duration of the Project (Planned and Actual)

Planned : 26th June 2019 – 25th November 2021 (30 months)
Actual : 26th June 2019 – 25th June 2022 (37 months)

4. Background

In response to the request submitted by the Government of the Socialist Republic of Viet Nam (Viet Nam), Japan International Cooperation Agency (JICA) has dispatched the Detail Planning Survey Team from the 1st October to 15th November, 2017 for the purpose of discussion on the technical cooperation project on "Project on Capacity Building for Cyber Security in Viet Nam" (Project).

Based on the Minutes of Meetings on the Detailed Planning Survey for the Project signed on 15th November 2017 between Ministry of Information and Communications of Socialist Republic of Viet Nam (Counterpart) and JICA, JICA held a series of discussions with the Counterpart and relevant organizations to develop a detailed plan of the Project. As a result of the discussions, both sides agreed on the matters referred to in the Record of Discussion (R/D) signed on 8th March 2019.

After R/D signing, the Project was initiated on 26th June 2019 with the dispatch of a long-term expert until 25th November 2021.

At the 2nd Joint Coordination Committee (JCC) on 14th August 2020, it was decided to extend the project until March 2022.

In January 2022, due to the delay of the equipment delivery, the Counterpart and JICA decided to extend the project term until June 2022.

Note that this report is a preliminary version that describes the information as of February 2022. Please refer to the final version supposed to be issued at the end of the project (June 2022).

5. Overall Goal and Project Purpose

Overall Goal : Cyber resilience for Vietnamese government is increased.
Project Purpose : Capacity of AIS for cyber security is enhanced.

6. Implementing Agency

Authority of Information Security (AIS), Ministry of Information and Communications (MIS)

II. Results of the Project

1. Results of the Project

1-1 Input by the Japanese side

(1) Amount of input by the Japanese side: 319 million Japanese Yen

(planned amount: 153 million Japanese Yen)

(2) Expert dispatch: 2 persons

- Long-term expert 1 person
- Short-term expert 1 person * Other short-term experts (4) supported online

(3) Receipt of training participants:

Training type	Number of Implementation	Number of participants
Local Training total	77	635
(Certification training)	(52)	(333)
(Custom training)	(25)	(302)
Training in Japan: Onsite	1	2
Training in Japan: Remote	8	13
Training in Indonesia	1	2
Total	87	652

* Training in Japan (online, onsite) is not a training program planned and implemented independently by the Project, but conducted by JICA HQ or the Japanese government. Priority was given to the participation of the Counterpart staff from the Project.

* Training in Indonesia is a training course in a third country related to the ongoing Project in Indonesia, "Project for Human Resources Development for Cyber Security Professionals" (22nd May, 2019 to 21st May, 2024).

(4) Equipment Provision: 78 million Japanese Yen

- DDoS Attack Mitigation System
- Malware Analysis System
- Equipment for support practice according to international standard Common Criteria

(5) Overseas activities cost: 128 million Japanese Yen
(Training: 92 million, Local activity: 36 million)

Major application items: Local staff, Awareness-raising material, local training, ISAC survey, Equipment for Common Criteria operation support, etc.

1-2 Input by the Vietnamese side

(1) Major counterpart assignment: 6 persons

- Project Supervisor: Vice-Minister of Ministry of Information and Communications 1 person
- Project Director: Director General (DG) of Authority of Information Security 1 person
  - DG of AIS changed in February 2020.
- Vice Project Director: Deputy Director General (DDG) of Authority of Information Security 1 person
  - DDG of AIS has moved to another position in November 2021. As of the end of January 2022, AIS DDG is vacant.
- Point of Contact (POC) of AIS: Legal and Auditing Division 3 persons

(2) Provision of offices, etc.: Project office, Facilities, Water supply, Electricity, Internet, etc.

(3) Other items borne by the counterpart government: 0 Vietnamese Dong

1-3 Activities (Planned and Actual)

Activity 1-1. (Output 1)

Clarify the required roles defined in SecBoK framework

< Past Information >

In the planning study of this project conducted in 2017, the 19 SecBok roles were divided into three levels of importance (high, medium, and low), and the policy was that AIS staff falling under the 14 roles assigned to the high and medium levels would be eligible for CDP. However, through interviews with AIS staff immediately after the start of the project, it was found that there was a lot of oversight in the 14 major roles, and as a result, CDP operations were started with a total of 22 roles, adding 3 roles to the 19 SecBok roles. The following table shows this classification. As a result, all the roles listed in this table were targeted.

Table 1 Role's classification

SecBok high / medium 14 roles	CISO, Commander, Triage, Incident manager, Incident handler, Vulnerability diagnostic consultant, Information security auditor, POC, Curator, Researcher, Solution analyst, Self assessment, Forensic engineer, Investigator
SecBok low 5 roles	Notification, Education / Awareness raising, Legal advisor, IT planning division, IT system division
Additional 3 roles	Licensing, Policy making, SOC (Security Operation Center)

Although the roles defined in SecBok are mostly suitable for departmental level, there are some opinions that the granularity of the roles is too large for individual roles within the organization and needs to be improved in order to assign appropriate training. In this regard, a short-term expert on career development planning has provided a review and suggestions in the CDP manual for reference. In this project, we used 22 roles based on SecBok shown in the table above.

Activity 1-2. (Output 1)

Develop a CDP for each staff based on SecBoK Framework

< Past Information >

Individual interviews of AIS staff started in August 2019 and CDPs for 36 staff were made. This was followed by the merging of VNCERT/CC into AIS in November, resulting in 67 staff being interviewed and CDPs being made by the end of 2019; AIS continued to actively recruit staff, increasing the number of staff covered to 106 by the end of the project. The following table summarizes this increase in the number of staff, along with the submission timing of the monitoring sheets.

Table 2 Number of Interview and Created CDPs

Monitoring Sheet Version	Number of new interviews	Newly created CDPs	Cumulative number of CDPs	CDP Target staff
Ver.1 (as of 30th December 2019)	67	67	67	**67**
Ver.2 (as of 30th June 2020)	25	25	(no data)	**80**
Ver.3 (as of 30th December 2020)	16	16	(no data)	**88**
Ver.4 (as of 30th June 2021)	20	20	(no data)	**106**
Ver.5 (as of 31st December 2021)	0	0	144	**106**
Project Completion Report (as of 30th October 2021)	0	0	144	**106**

The difference between the Cumulative number of CDPs and the CDP target staff corresponds to the number of retirees.

The action of "Making a CDP" is filling out the results of the interview in an Excel based CDP form. The actual CDP form (completed example) is attached to the ANNEX. The items to be filled in the CDP form are listed in the following table.

Table 3 CDP fill-in items

CAREER DEVELOPMENT PLAN	
1	Division & Title
2	Job Description, Responsibility
3	Assigned Security Role(s)
4	Required Knowledge and Skills for the Roles (General description)
5	Knowledge and Skills to be acquired or improved
6	Training plan, progress and result
	Course Title, Couse Code, Vendor, Course Provider, Planned Month

	Attending Date, Number of Hours, Certification, Progress, Remark
PROGRESS REVIEW	
1	Review 1
2	Review 2
3	Review 3
4	Review 4

Since it is not easy to maintain and update the CDPs consisting of over 100 Excel files, we also built and operated a CDP database for centralized management of CDPs. Details of the CDP database is described in the separated document “CDP manual”.

Activity 1-3, 2-1, 3-1. (Output 1,2,3)

Develop a training course plan for high prioritized roles defined in SecBoK Framework

< Past Information >

At the beginning of the project, it was assumed that the training would be assigned according to the SecBok roles described in the staff’s CDP to meet the required KSA (Knowledge-Skill-Ability). However, in actual operation, as described in Activity 1-1 (Output 1), we faced the problem that the roles defined in the SecBok were not appropriate for mapping individual roles within the organization because the granularity of the roles was too large, although they were almost sufficient for department level. There are two aspects to this problem as shown below.

1) For example, in the category of Education / Awareness raising, the staff who plan and develop cyber exercises need to have advanced knowledge of cyber attack offense and defense, as well as infrastructure building skills. On the other hand, those in charge of Child Online Protection are required to have knowledge of media strategy and school education rather than such specialized technical skills. In other words, the Education / Awareness raising category covers too wide a range to specify the knowledge and skills required for individual staff.

2) Roles assigned to a staff often result in multiple SecBok roles. For example, even a staff with only three roles such as Incident handler, Vulnerability diagnostic consultant, and Forensic engineer should take almost all cybersecurity training courses because of KSA-based mapping rule. This is due to the large granularity of the SecBok roles and the large amount of KSAs that correspond to each role.

In order to address these issues, in addition to the SecBok role, we clarified the following items through interviews and included them in the CDP to provide reference information for each staff member when making their training plans.

- Job Description, Responsibility
- Required Knowledge and Skills for the Roles (General description)
- Knowledge and Skills to be acquired or improved

In other words, in this project, the basis of the training plan for each staff member was the SecBok role and individual job and skill analysis. To make this procedure more clearly and logically, short-term experts in career development planning have suggested hat the basis of the training plan should be sought from the NICE framework that was the basis of SecBok. The topic will be described in the separated document "CDP manual".

Activity 1-2, 2-2, 3-2. (Output 1,2,3)

Conduct training

The total number of courses is 87. In general, the training was completed as scheduled, which can be highly efficient. See ANNEX for details of the training conducted.

Activity 1-5, 2-3, 3-3. (Output 1,2,3)

Review CDP (e.g. every six months)

The planned review procedure is as follows. The project team constantly conducts the CDP review every 6 months, so the efficiency of CDP review activity is high.

1) Preliminary questionnaire and interview with the superiors of targeted staff
2) Update CDP and modify the training plan

The following table shows the time frame and number of targets for the CDP review.

Table 4 Number of CDP Review

CDP Review	Term	Number of Target	Note
1st review	May – June 2020	57	one person is retired at the end of June
2nd review	November 2020 – January 2021	82	-
3rd review	May – July 2021	82	10 staff who were no longer eligible due to turnover or promotion at the time of the review at that time.
4th review (Final)	29th November 2021 – 29th December 2021	104	-

The table below summarizes the responses to the questions asked to the target staff in the CDP review.

- **Update of your job role or daily tasks from last interview**

	No update	Updated	Total	Note (main reason, etc.)
1st review (2020)	16	41	57	Organizational restructuring was still ongoing since VNCERT/CC joined AIS in November 2019. Although details of the changes in each person's duties were not provided in the document, it was found that the roles and tasks of the staff are constantly changing. We believe it is important to repeat the review of roles and tasks at the time of the CDP review to provide training to meet the staff's changing needs.
2nd review (2021)	46	27	73	the role in the department has increased, the role of the staff has changed, more duties assigned (but same position).
3rd review (2021)	68	14	82	the role in the department has increased, the role of the staff has changed, more duties assigned (but same position).
4th review (final)	95	9	104	The examples of the updates are as follows: • Secretary Department (Ministry Office), Secretary of Vice Minister • My daily tasks have increased from the last interview, joined more projects at work • Solution and architect for software and security software • Deputy head of the division • Deploy more services activities in 2022 related to drill on the real systems and evaluation the maturity of CSIRTs in provinces and organizations • General management and development of information security services in the region

- **Challenges for your daily tasks or job roles**

	No challenges	Have challenges	Total	Note
1st review (2020) ( ) shows the answer of superiors	22 (1)	35 (13)	57 (14)	Almost all divisions have challenges specific to their duties. The division that responded that there were no challenges was the Incident Monitoring Division of National Cyber Security Center (NCSC). However, the interviewee (division head) is likely aware that the division lacks capacity, as he expressed the need to improve their monitoring and incident response capacity in the interviews. It is important to note that all of the divisions perceive lack of competence. The project should provide appropriate training to address these challenges.
2nd review (2021)	61	12	73	Most of the comments are about the lack of human resources and skills. While the project cannot encourage to hire more staff, we will continue to provide AIS with the systematic training methods using the CDP that we are implementing through the project.
3rd review (2021)	59	23	82	Software architecture, Human Resources allocation and development, especially in Da Nang and HCMC, Accreditation skills following procedures built from international and national standards, Difficulties in designing policies in new area, protecting children on internet, Foreign Language, Scenario planning for cyber security exercise, Web application pen-testing, Mobile application pen-testing, Forensics
4th review (final)	85	19	104	The examples of the challenges are as follows: • English in Cybersecurity • Malware analysis • Knowledge and plan to work more effectively • Limited knowledge, not much experience • Lack of cybersecurity/information security knowledge • Software architect & system architect • Build CTF LAB • Experience in making policy • Work management skills, Collaboration skills, Quantitative skills, Negotiation, Public – speaking, Comprehensive skills • Lack of information on regulation and policies in the field of Information security, data protection • Knowledge about inspection, security evaluation • Work from remote site • Working more in Web Security • General skills

- **Effects of training and behavioral changes (for trainees)**

	Improved	Negative effect	Not feel	Don't know	Total
1st review (2020)	30	0	9	1	40
2nd review (2021)	56	2	7	8	73
3rd review (2021)	67	4	6	5	82
4th review (final)	See the table below, as the answers allow for duplication.				104

- 2nd CDP Review:

The reasons for the two respondents who chose " I feel negative effect in my daily work as a result of the training " are as follows:

- The training was not excellent and did not lead to a solid sense of confidence.
- More practical contents in the PMP training were expected.

- 4th CDP Review:

1	**Become more confident**	57
2	**Broader scope of work**	33
3	**Career path becomes clear**	30
4	Better recognition by supervisor	12
5	Promoted	7
6	Nothing has changed	7
7	Have negative impact	2

- **What did your attitude or way towards work change after you participated in the training?**

From the comments of the 2nd and 3rd CDP reviews, many of the participants gained knowledge of security technology, business English, and project management from the training and applied it to their work. (See ANNEX for each comment)

- **(4th review questions). Update of your request for acquiring knowledge or taking courses / certificates**

- Media and communication course
- Program/Project Management, Project Management Professional (PMP)
- Advanced Malware Analysis
- Course for Software engineering career path
- Leadership skills
- Advanced English in Cybersecurity/English for IT
- Information security policy
- ISC2's Certified Information Systems Security Professional (CISSP)
- EC-Council's course (CEH, CHFI, CNP)
- SANS (GREM - GIAC Reverse Engineering Malware)

- Offensive Security (OSWE, OSEP, OSED)
- Cloud security: GIAC Cloud Security Automation / ISC2's Certified Cloud Security Professional (CCSP)

- **(Question to Division Head) Did your staff's attitude or way towards work change after he/she participated in the training?**

  During the first review, each trainee was asked to answer the questions, but after the second review, each supervisor obtained the answers.

	Improved	Negative effect	Not feel	Don't know	Total
1st review (2020) ( ) shows answer by the superior	30 (30)	0 (0)	9 (4)	1 (1)	40 (35)
2nd review (2021)	11	1	0	0	12
3rd review (2021)	10	2	0	0	12
4th review (final)	17	1	0	0	18

- **(4th review question) Do you want to continue using the CDP-based training planning method after the JICA project is over?**

Yes	95
No	9
Total	104

The examples of the reasons are as follows:

[Yes]

- Because it provides me with a clearer career path which in turn help me efficiently get indispensable knowledge and qualifications for my job. CDP is a useful tool to help me map and track my career development strategies. CDP-based training seems like a great method to build a foundation for my career path. Because I think it's a suitable roadmap for me to improve skill and experiences.
- The training courses are very useful, play a huge role in the development of a business or organization. It helps me to improve necessary skill. It makes the training course be useful for our daily work. Because I can have an overall look through the need of knowledge and skills that a staff in cyber security need to improve step by step.
- Because I can track my own progression throughout the year.
- This project greatly improves the quality of human resources development in AIS. I hope this project can be extended. The CDP-based training planning method can be used for internal training
- Because I have chance to use English, practice and learn more about cybersecurity and how to manage projects.

[No]

- ➢ The time fund to allocate to improve knowledge is currently not arranged.
- ➢ That all I need to learn, because my daily task is accounting.
- ➢ The learning path is not transparent to learners, Feedback is basically a formality.
- ➢ It is very basic. It's not enough to do my job.

- **(Question to Division Head) What do you think of CDP? Is it useful for your organization and your management?**

	Yes, it is useful but need improvement	Yes, it is useful very much.	Total
1st review	8	6	14
2nd review	1	11	12
3rd review	1	11	12
4th review (Final)	15	3	18

- **Q. Do you have any ideas for improvement of CDP method?**

- ➢ The courses are all very good, following the learning needs of each student. However, if the study time is extended, it will be more effective.
- ➢ More time for a training course and divided into batches so that students can better grasp the knowledge.
- ➢ In my opinion, CDP is already quite effective method. This CDP method is useful and excellent to manage training orientation and skills enhancement. I have not had any more ideas for improvement at the moment.
- ➢ Viet Nam should build our security body of knowledge base on some national SecBoK (ie Japan, US, etc.).

Open more practical courses.

Activity 1-6. (Output 1)

Plan and conduct training for policy maker

The following table shows policy-making related courses conducted since the beginning of the project.

Table 5 Policy-Making related training courses

No	Course Name	Date	Venue	Area
1	Training in Japan: Capacity Building in Policy Formation for Enhancement of Measures to Ensure Cybersecurity in ASEAN Region	January to February 2020	Onsite	Japanese policies and strategies
2	Cybersecurity Policy Making Online Seminar by Japanese Ministries and University	19th – 21st July 2021	Online	Japanese policies and strategies
3	Awareness-Raising Online Seminar	30th, 31st August – 1st September 2021	Online	Awareness raising, COP
4	Training in Japan: Capacity Building in International Law and Policy Formation for Enhancement of Measures to Ensure Cybersecurity	25th October – 3rd November 2021	Online	Japanese policies and strategies, Internet and cyber space governance, UN 11 Norm, etc.

Activity 1-7. (Output 1)

Develop/localize awareness raising materials

The activities related to awareness-raising are divided into video creation, portal website development, branding kit and survey and training and consulting by JICA experts.

1) Video Creations

The following animation videos for youth and children were created during the project period.

- 1st animation video

Theme	Staying vigilant with strangers in virtual space, especially on social media
Target	Children studying in secondary schools (from 11 to 14 years old)
Duration	180s
Creation company	KYX
Quality	Full HD (1920x1080)
Development Term	August 19th 2020 – December 9th 2020

- 2nd animation video

Theme	Save the Children on Internet
Target	Children studying in primary schools (from 6 to 10 years old)
Duration	180s
Creation company	DeeDee
Quality	Full HD (1920x1080)
Development Term	December 28th 2020 – 23rd March 2021

- 3rd animation video

Theme	Introduction an Online Contest of Information Security for students
Target	Children studying in secondary schools (from 11 to 16 years old)
Duration	Full version (max 180s) Short version (~1 min)
Creation company	DeeDee
Quality	Full HD (1920x1080)
Development Term	3rd May 2021 – 14th June 2021

2) Branding Kit

It aims to make the Viet Nam Child Online Protection (VN-COP) Network, which is being established through the cooperation of relevant ministry departments such as AIS, Ministry of Public Security, Ministry of Education and Training, Ministry of Labor - Invalids and Social Affairs, as well as many international and non-governmental organizations, into a trusted community, making this community easy and immediately recognizable to children and their parents. The project developed a branding kit (design) on COP in cooperation with MỸ THANH Corporation to make the activities of AIS on COP widely known to the public. The outputs are as follows:

- Core part of the Brand Kit (Identity Kit)

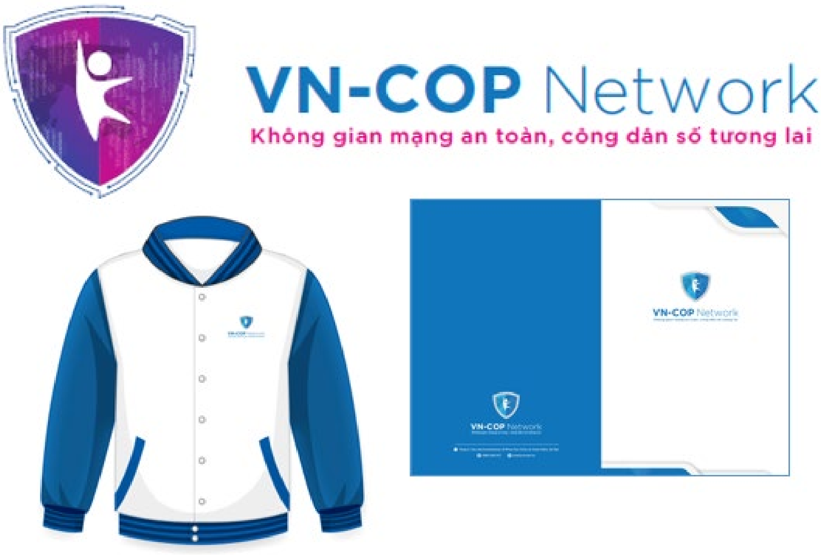
  Logo, Website template, Social media, Slogan, Uniform Design

- Office Application of the Brand Kit

  Certificate Design, Business card Design, Letterhead Design, Envelope Design, File folder Design, Slide template Design

- Gift Set Design

  Souvenir medal/ badge, Other gifts with logo of VN-COP Network

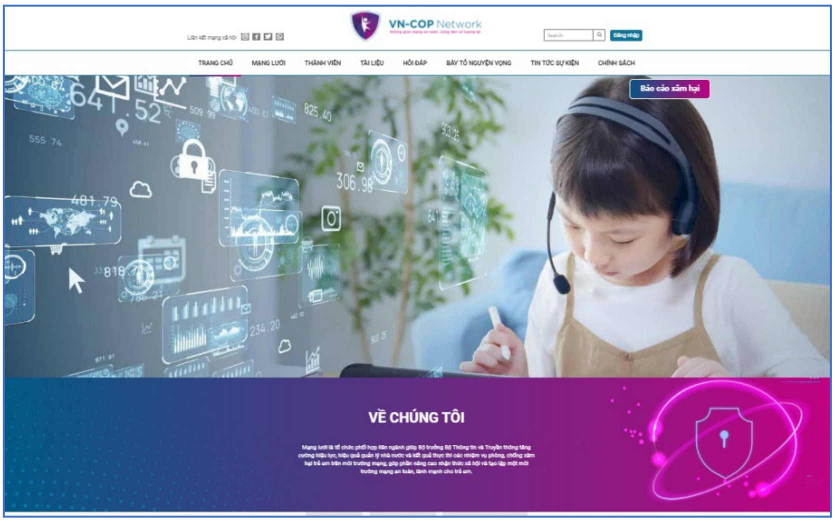


3) Portal Site Development

In the project, consulting on the development of the COP portal site and discussion of the system requirements with AIS were conducted from April to June 2021. Based on the results, the portal site with the following services was developed by the agile method in cooperation with the local company SolidTech.

1) Registration, 2) Legal Document Publication, 3) Answer Questions and Inquiries, 4) Feedback and Aspirations of Parents and Children, 5) News and Events, 6) User Data Privacy Policy (AIS policy setting), 7) Reporting

URL: https://vn-cop.vn/

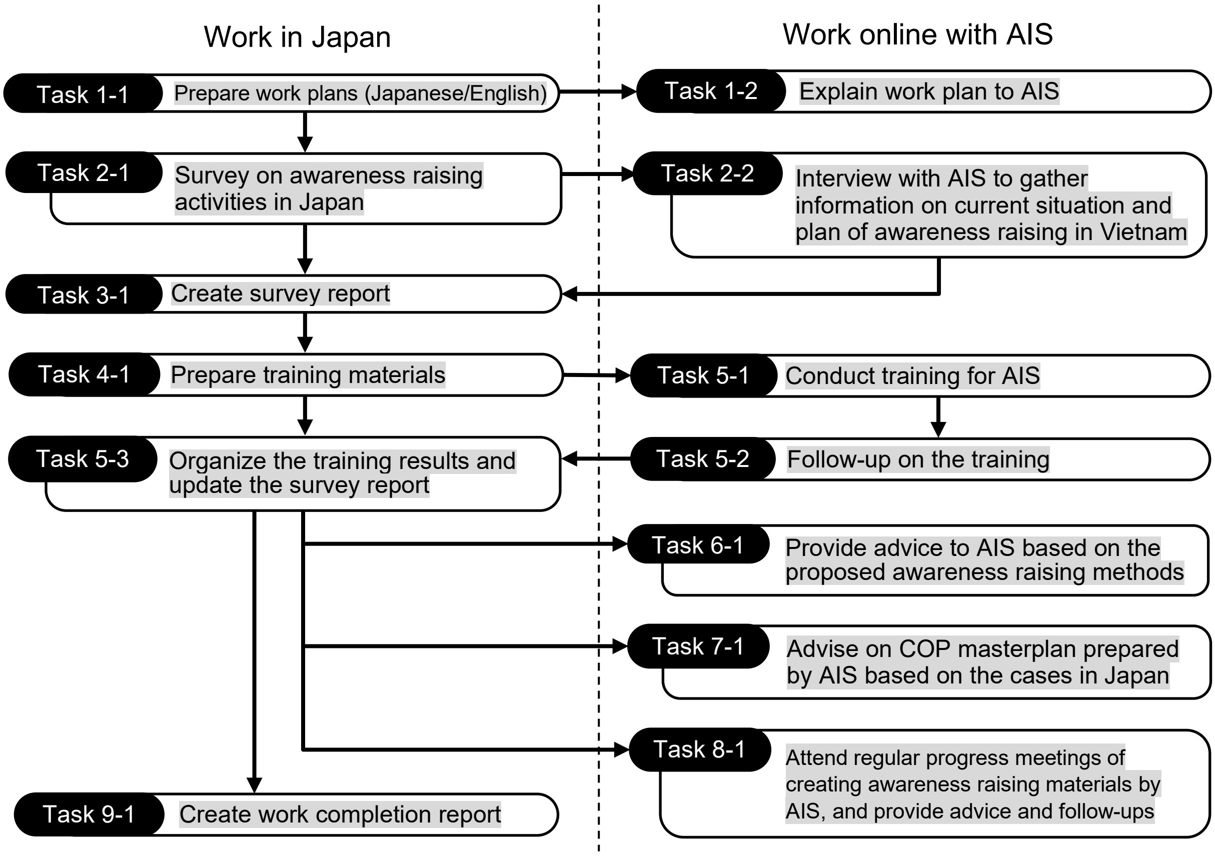


VỀ CHÚNG TÔI

Mạng lưới là tổ chức phối hợp liên ngành giúp Bộ trưởng Bộ Thông tin và Truyền thông tăng cường hiệu lực, hiệu quả quản lý nhà nước và kết quả thực thi các nhiệm vụ phòng, chống xâm hại trẻ em trên môi trường mạng, góp phần nâng cao nhận thức xã hội và tạo lập một môi trường mạng an toàn, lành mạnh cho trẻ em.

4) Awareness-Raising Expert

At the 2nd JCC in August 2020, without changing the original PDM framework, experts were added with the activities of “1-4. Conduct training” and “1-7. Develop/localize awareness-raising materials”. Awareness-raising activities on cybersecurity in Japan and necessary marketing methods for promoting the activities were thoroughly researched. The results of this research were summarized into the report of survey results and converted into training materials for the training implemented for AIS staff. Based on the result of the training, the expert team implemented the follow-ups for the additional survey and the recommendation to AIS. The initial plan was to visit the project site in Viet Nam to conduct the actions. But due to COVID-19, all planned on-site activities had to be replaced with online activities connecting the project site with the awareness-raising experts in Japan.


Work in Japan
Work online with AIS
Task 1-1 Prepare work plans (Japanese/English)
Task 1-2 Explain work plan to AIS
Task 2-1 Survey on awareness raising activities in Japan
Task 2-2 Interview with AIS to gather information on current situation and plan of awareness raising in Vietnam
Task 3-1 Create survey report
Task 4-1 Prepare training materials
Task 5-1 Conduct training for AIS
Task 5-3 Organize the training results and update the survey report
Task 5-2 Follow-up on the training
Task 6-1 Provide advice to AIS based on the proposed awareness raising methods
Task 7-1 Advise on COP masterplan prepared by AIS based on the cases in Japan
Task 8-1 Attend regular progress meetings of creating awareness raising materials by AIS, and provide advice and follow-ups
Task 9-1 Create work completion report

- **Task 1-1 Prepare work plans (Japanese/English)**

We have obtained information on the project from JICA headquarters, chief advisor, short term experts, and long-term expert to understand the past efforts of the Vietnamese government on cyber security and the overall activities of the project, and then have prepared the work plans in Japanese and English. Japanese version was presented and explained to JICA for approval.

- **Task 1-2 Explain work plan to AIS**
- **Task 2-2 Interview with AIS to gather information on current situation and plan of awareness raising in Viet Nam**

The explanation of work plan and the interview to AIS were done at the same time as an online meeting on July 30th, 2021.

Date & Time	July 30th, 2021 9:00-11:00 (Vietnam time)
Participants	AIS: 7 including Deputy Director General JICA: 3 including 1 awareness raising expert
Main Points	● Work plan was explained and AIS side agreed with the content of plan ● AIS side explained about the current status of master plan 2020-2025 that includes awareness activities scheme. ● The strategy has 3 focuses: 1. Mass media channel where they believe most of the youth are landing as targets. 2. Fostering the domestic products and services serving the creative cyberspace for children

	3. Developing the educational materials and implementing such stuffs into the school system ● Facebook Messenger, Viber, Instagram, Zalo are popular instant message app in Vietnam. YouTube is still popular besides the social media, especially for the children, but they cannot judge whether the content is good or bad without support from the parents. ● IT subjects are integrated in the current educational curriculum but the influence of massive information from SNS is overwhelming. From the scheme of Child Online Protection (COP), the target of communication should not only be children, but also their parents. Hotline is needed for children because children may not prefer to directly talk to their parents. ● Vietnam is trying to establish the COP network including the schools as a top-down method. This network is not only for the school system, but also for the parents, children themselves and front-line staffs (social services employees). ● There is very limited cooperation between Government and private sectors in Vietnam. However, the scheme is also trying to foster the domestic products and services toward the children. ● The current master plan approved by the Prime Minister last year mentions about the 64 provincial Government to take their responsibility. Inside MIC, they have also got the monitoring plan to follow up the strategy. ● As for the content of planned training, the proposed plan is fine. AIS would like to know the "know-how" of applying the Japanese policy in daily operation of awareness raising. For the education materials, it seems the animations are strong advantages, for example. It would be helpful if there is some content about prevention of child abuse.

- **Task 2-1 Survey on awareness raising activities in Japan**

Information on awareness raising activities in Japan have been surveyed in order to develop training materials. Contents of these information sources are summarized in the survey report.

- **Task 3-1 Create survey report**

The results obtained from the above survey were organized, and the numerical information were analyzed using statistical methods, and a survey report were prepared in English.

- **Task 4-1 Prepare training materials**

Training materials including practice materials were developed based on the result of survey in English. The materials contain comprehensive reference information on where to obtain Japanese awareness raising/educational materials that have been found in the survey.

- **Task 5-1 Conduct training for AIS**

Three-days training was conducted from August 30th to September 1st 2021 through online method by using the teaching materials developed in the above activities. Number of participants was 11 staffs from AIS.

The purpose of the seminar was also related to the use of these materials and aimed at the following.

- To understand the experience of dissemination and awareness activities in Japan and to consider the educational materials and activities applicable to Viet Nam.
- To learn how to apply marketing theory to dissemination and awareness activities related to cyber security

At the end of each day of training, Q & A session was conducted, and efforts were made to provide feedback on the following day. Questions and requests from participants that require additional survey were brought back to the experts for further research and answered in the follow-up activity described in the next section.

- **Task 5-2 Follow-up on the training**

During the training course, there were several requests raised by the participants for additional information and contents such as shown below, and the experts prepared additional information and materials. This additional information was incorporated in updated teaching materials as well as updated survey reports.

- National budget of Japan allocated to cybersecurity awareness raising
- List of links to information introduced in the training
- Detailed information on "Cybersecurity Helpers Service Project" by IPA

- **Task 5-3 Organize the training results and update the survey report**

Based on the results of the feedbacks obtained during the training as well as the result of subsequent online discussions with AIS, the experts organized the training results and updated the survey report.

- **Task 6-1 Provide advice to AIS based on the proposed awareness raising methods**

Based on the theories and strategies for effective awareness raising activities that were transferred during the training, the experts made necessary recommendations for future awareness raising activities in a follow-up online meeting on September 29th as shown below.

Date & Time	September 29th, 2021 11:00-12:00 (Vietnam time)
Participants	AIS: 3 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	The expert team has provided advice on the following topics. ● The 4th awareness raising video ● Development of branding kit ● Development of COP portal site AIS and JICA team has discussed on the following topics. ● Plan to support COP master plan – Draft is available in early October 2021 ● Extended support from awareness raising experts until January 2022

- **Task 7-1 Advise on COP masterplan prepared by AIS based on the cases in Japan**

The expert team received the draft COP master plan from AIS on October 8th, 2021. The expert has read the full content and provided various comments and suggestions to it, and then returned the commented version back to AIS. The AIS acknowledged the comments and suggestions during the next meeting (see later) and told the expert team that they will examine these and act properly.

- **Task 8-1 Attend regular progress meetings of creating awareness raising materials by AIS, and provide advice and follow-ups**

The expert team has attended the following regular meetings to provide advice and follow-ups on the awareness raising activities of AIS. In each meeting, there are several requests from AIS regarding additional information in Japan as well as the recommendations to their activities.

Regular meeting with AIS on awareness raising activities #1

Date & Time	November 5th, 2021 11:00-13:00 (Vietnam time)
Participants	VNCERT/CC: 4 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	Review of the COP masterplan (The expert has already sent commented version before). ● The expert recommended to add "Child emergency call" telephone number as well as email/SNS contacts like in Japan. ● Vietnam has the 111-call center for similar purpose, but people do not remember well about it. Regarding cybersecurity education contents ● Since there is no cybersecurity education in Vietnam, AIS is looking for the focused and consolidated contents for awareness raising of each target age group. ● Three content types in Japan now: message based, storytelling based and case study.

Regular meeting with AIS on awareness raising activities #2

Date & Time	December 6th, 2021 14:00-15:00 (Vietnam time)
Participants	VNCERT/CC: 4 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	The expert prepared and sent a material containing the answers to the request made in the previous meeting (“Information Moral Education - Model Curriculum”). ● Enhancing the management ability is the answer for the question about how to manage many tasks with limited time and resources. ● It is hard to create KPI for evaluating contents for each target age group. The expert created sample CyberSec KPIs so it would be a reference. ● Evaluation should be done hired consultant company, but it does not have to be expensive foreign consultants.

Regular meeting with AIS on awareness raising activities #3

Date & Time	January 6th, 2022 14:00-15:00 (Vietnam time)
Participants	VNCERT/CC: 3 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	The expert prepared and sent a material (before the meeting) containing the answers to the request made in the previous meeting (“Government control on applications for children in Japan”). ● There is no government control on applications for children in Japan, but some industry associations do the screening. ● AIS is aiming to establish the criteria to evaluate the application, games to ensure the child protection policy. Game rating or equivalent criteria is supposed to be issued by Government, but the actual evaluation may be done by other entity. Such request is to protect children from abusive activities via the reporting system. ● No update for COP masterplan Questions of AIS to the experts (to be answered in the next meeting) ● Is there any fee required for evaluation from the organization such CERO? What is their evaluation criteria? Who will do the evaluation? ● Is there any example of evaluation criteria (such as checklist or template) in Japan that can be obtained? ● Recently, VNCERT/CC has been assigned more tasks about the communication e.g., YouTube and FB channel to gain 100,000 followers/subscribers for each channel. How to do that with the limited budgets? Now they have the support from Google, but they are looking for the expert’s support to build such plan as adapting KPIs.

Regular meeting with AIS on awareness raising activities #4

Date & Time	January 24th, 2022 14:00-15:40 (Vietnam time)
Participants	VNCERT/CC: 4 from inspection division JICA: 5 including 2 awareness raising experts
Main Points	The expert team prepared and sent a material containing the answers to the requests made in the previous meeting (updated version of "Government control on applications for children in Japan", presentation on how to design KPI for reaching 100,000 followers/subscribers). ● CERO is for game evaluation only, but how should we control PC applications? ● There is no rating system for general application in Japan except for some. There are filtering software for mobile phone, but kids tend to bypass it. The expert did comprehensive presentation on how to reach 100,000 followers/subscribers including analysis of existing YouTube videos on COP in Japan and the setting up of KPI.

- **Task 9-1 Create work completion report**

The results of all activities were compiled into a work completion report and submitted to JICA.

Activity 2-3. (Output 2)

Expand reactive infrastructure (e.g. DDoS attack mitigation, malware analysis) in AIS

The total number of equipment provided by the project through activities 2-3 and 3-4 is as follows.

Package Type	Hardware	Software	Total
DDoS attack mitigation system	98	0	98
Malware analysis system	29	52	81
Evaluation lab system	19	3	22
Total	146	55	201

Note: The TSUBAME sensor software provided by JPCERT/CC is not included in the above, as it is not a direct activity of the project.

The DDoS attack mitigation and malware analysis systems were procured as reactive infrastructure equipment through activity 2-3.

- **DDoS Mitigation System**

The equipment (servers, network equipment, and accessories) related to the DDoS attack mitigation system was delivered on 13th March 2021. It is expected that these devices will be able to handle DDoS attacks up to approximately 75 Gbps. On 3rd November 2021, the project team visited the AIS office and server room to ensure they were properly installed. At that time, the project team found that 74.5% (73/98) of the equipment was in use, and there were no problems with the operational management status of the installed equipment.

Since all the equipment's installation and operation has not been completed, AIS plans to start the operation as soon as possible.

- **Malware Analysis System**

  At the 2nd JCC on 2nd August 2020, additional equipment was added to the list of malware analysis equipment as the project term was extended. The Project Document, including the updated list of equipment for the malware analysis system, was approved on 16th July 2021. The procurement was originally scheduled to start during 2020, but this approval delayed the start of the procurement by several months (the contract with KDDI Viet Nam Corporation, the equipment vendor, was signed on 15th November 2021). Most of the malware analysis-related equipment is scheduled to be delivered by the end of March 2022. But due to COVID-19, some of the equipment will be delivered after April 2022.

  With the cooperation of JPCERT/CC, training on malware analysis was held in December 2021, and a meeting on the construction of the environment for malware analysis equipment was held in February 2022.

Activity 3-4. (Output 3)

Expand proactive infrastructure (e.g. network monitoring, equipment for support practice according to international standard Common Criteria) in AIS

DDoS attack mitigation systems and Security Evaluation Equipment (equipment for support practice according to international standard Common Criteria) were procured as proactive infrastructure through activity 3-4.

- **DDoS Mitigation System (network monitoring)**

  See Activity 2-3. (Output 2).

- **Security Evaluation Equipment**

  The project was extended at the 2nd JCC on 2nd August 2020, and the much-needed security evaluation equipment was added. The Project Document, including the list of evaluation equipment, was approved on 16th July 2021. Procurement was originally scheduled to begin in 2020, but this approval delayed the start of procurement by several months (contract with equipment vendor KDDI Viet Nam Corporation was signed on 15th November 2021). Most of the equipment is scheduled to be delivered by the end of March 2022. But due to COVID-19, some of the equipment will be delivered after April 2022.

  As for security evaluation, training on Common Criteria was conducted several times. In addition to the training for proper operation of the equipment (security and evaluation procedures), the following documents were prepared, and the AIS was trained from September 2021 to January 2022 with the cooperation of local companies and Vietnamese experts.

  - Lab security manual

- Lab evaluation procedure
- Evaluation Technical Report (ETR) Template

- **TSUBAME**

  Although not within the scope of this project's activities, the project team assisted in installing the Asia Pacific Internet Threat Monitoring System (TSUBAME)[1], which has been operated by JPCERT/CC since 2008, on AIS. For many years, Viet Nam was not a member of TSUBAME, but at the end of 2020, through this project, VNCERT/CC decided to join TSUBAME. After installing the TUSBAME sensors, observation trends and information from member countries based on TSUBAME information and alerts for incidents were shared, contributing to the improvement of the AIS threat intelligence collection capabilities.

2. Achievements of the Project

2-1 Outputs and indicators

This section will describe the degree of achievement and effectiveness of the output (the validity of the causal relationship between the output and the project objective). The results of each output are as follows.

Output 1-1: CDPs are set.

The initially planned number of CDP targets was 40. Finally, 106 CDPs are set based on the individual interview (total of interviews was 139). The increase in the number of CDPs is due to the request from AIS to increase the number of training participants and the increase in the number of personnel due to the integration of VNCERT/CC, which was an independent organization under MIC, into AIS in November 2019. Created CDPs by the project were approved by the target's supervisors.

The last addition to the CDP was closed in July 2021, but due to the large number of requests from AIS, a new CDP was created until October 2021. In the latter half of the project, AIS staff who had not prepared the CDP were also allowed to participate in the training if there were slots available.

Therefore, the output 1-1 ***"CDPs are set"*** is achieved.

Outputs 1-2, 2-1, 3-1: Capacity of the trainees is improved.

Overall, pre-test scores, post-test scores, online learning scores, and certification exam scores increased in most training compared to pre-test scores. Also, trainee's and trainers' training evaluation was high in the post questionnaire survey. There has been a steady increase in the number of trainees passing the international certification examinations, although the target passing rate is not set as a goal. As a result of the CDP review, most trainees and supervisors feel that the

[1] https://www.jpcert.or.jp/english/tsubame/

training has changed their mindset and improved their daily work (e.g. infrastructure, monitoring, and pen testing).

Therefore, the output 1-2, 2-1 and 3-1 "*Capacity of the trainees is improved*" are achieved.

The project team evaluates each certification training step by step as follows.

1) Reaction : Obtain feedback from trainees if the participants were pleased with the training.

2) Learning : Obtain pre and post-test results what the participants learned in training.

3) Results : Check if the participants change their behavior or improve their daily work based on what they learned. Check if the change in behavior positively affected the organization or cybersecurity resilience in Viet Nam.

(1) Reaction: Feedback from trainees

At the end of each certification training, a questionnaire was taken to measure the trainee's satisfaction. The project team concluded that the trainees' satisfaction with the training was high from these results. (See ANNEX)

(2) Learning: Pre-test, post-test and certification exam

A comprehensive evaluation for measuring the improvement of the trainees' actual knowledge will be conducted by comparing the pre-test and post-test, the online self-learning state after the training, and the certification exam status. For the international certification-related courses, a comparison of confirmation tests before and after the training, the pre-test and online learning scores, and the status of certification exams are shown in ANNEX. Since the grade of each test is different, a simple score comparison is meaningless.

[Intensive Training]

"Planned Num. of trainee" refers to the number of participants planned before the training, and "Actual Num. of trainee" refers to the number of people who attended the training. Since some people could not participate immediately before or during the training, we would like to improve the training procurement process so that the number of participants does not decrease after the course. Even a cancellation happens, the same training company can be asked to provide the next training session so that no additional costs are incurred for the canceled slot. "Increased point (pre vs. post-test)" is a comparison of the results of the pre- and post- tests (comparing the difference after the percentages are calculated), which shows that the training has increased (temporarily) knowledge. The pre- and post-tests for OSCP, LPT and OSWE were not simple multiple-choice questions, but they were exercises, so a simple comparison is meaningless.

[Online Practice]

“Actual Num. of trainee” refers to the number of trainees who tried to practice online. “Increased point (pre vs online-test)” compares pre-test and online practice scores.

Online Practice / Attendees	**62.5%**

[Certification Exam]

“Increased point (pre vs exam test)” compares pre-test and exam scores. Comparing the pre-test results with the certification exam shows a significant improvement over the post-test. The key ratios are as follows.

1)	**Examinee / Attendees**	**55.6%**
2)	**Pass / Examinee**	**79.5%**
3)	**Pass / Attendees**	**44.1%**

The project does not aim to pass certification exams, except for specific training such as OSCP or OSWE. However, it is expected that studying for the certification exams will help the trainees to retain what they have learned in the intensive training. Therefore, the project will make announcements before and after the training, encourage participants to take the exam via e-mail, and make recommendations during CDP reviews to ensure that the ratios of the above three points increase.

In the PDM, the pre and post-test results and the score comparison between pre and online learning are used as a complementary quantitative measure to determine the achievement of the output. Since the project's main objective is not to pass the exam, the exam results are treated as a reference.

From the above, it is concluded that the short-term effects of the training have been fully achieved.

Outputs 1-3: Number of awareness materials is increased.

At the beginning of the project, the target number of awareness materials was not set. Because the targets and contents of the materials had not yet been determined, it was assumed that it would take time to consider them. The final deliverables are as follows.

Therefore, the output 1-3 “Number of awareness materials is increased” is achieved.

Deliverables	# of Deliverables	Contents
Awareness videos	3 videos	Title: 1) Staying vigilant with strangers in virtual space, especially on social media 2) Save the Children on Internet 3) Introduction an Online Contest of Information Security for students
Branding Kit	1 set	• Core part of the Brand Kit (Logo, Website template, Social media, Slogan, Uniform Design) • Office Application of the Brand Kit (Certificate Design, Business card Design, Letterhead Design, Envelope Design, File folder Design, Slide template Design) • Gift Set Design (Souvenir medal/ badge, Other gifts with logo of VN-COP Network)
COP Portal site	1 portal site	Service: Registration, Legal Document Publication, Answer Questions and Inquiries, Feedback and Aspirations of Parents and Children, News and Events, User Data Privacy Policy, Reporting

Outputs 1-4: The developed materials are used.

Three animated videos created by the project are now utilized on the following website

- *Học sinh với An toàn thông tin*

  https://www.youtube.com/channel/UCz39i69Rz9nbqzffczICqsw

The number of views of the video is as follows.

Video name	Published Date	Number of Views	Link
1st video (Câu chuyện Công chúa và Thạch Sanh)	2021/05/26	55	https://www.youtube.com/watch?v=kSPXEgVa7SU&t=101s
2nd video (Bảo vệ trẻ em trên mạng)	2021/05/25	133	https://www.youtube.com/watch?v=Zsfrgmdh6wg&t=11s
3rd video (Cuộc thi Học sinh với ATTT 2021)	2021/06/25	721	https://www.youtube.com/watch?v=ja1tQ8saJAo

The third video was also shown at the Security Day by Vietnam Information Security Association (VNISA), (25th November 2021).

Through the Awareness-raising seminar on dissemination and awareness-raising, JICA experts provided guidance on dissemination and awareness-raising strategies and effectiveness measurement methods for Viet Nam based on Japanese knowledge. However, the knowledge was not utilized well by AIS

In summary, the videos the project developed have already been uploaded and used, but AIS has not effectively utilized all of the knowledge provided by the project.

Therefore, the output 1-4 “*The developed materials are used*” is partially achieved.

Outputs 1-5: Acquired knowledge for practice of policy making is utilized

The following are the policy-making related training courses that have been conducted. According to the questionnaires after each course and the CDP reviews, the target staff seem to have acquired knowledge of each policy through the courses, but they have not been utilized as actual policy-making activities in Viet Nam.

Therefore, the output 1-5, “*Acquired knowledge for practice of policy making is utilized*,” has only been partially achieved.

Table 6 Utilization status of policy-making related training courses

No	Course Name	Examples of the use of acquired knowledge
1	Training in Japan: Capacity Building in Policy Formation for Enhancement of Measures to Ensure Cybersecurity in ASEAN Region	To be utilized
2	Security Policy Making Online Seminar	To be utilized
3	Awareness-Raising Online Seminar	Used in COP policy formulation and implementation
4	Training in Japan: Capacity Building in International Law and Policy Formation for Enhancement of Measures to Ensure Cybersecurity	To be utilized

Output 2-2: Reactive infrastructure is improved

The equipment that improves the Reactive service is a DDoS attack mitigation system and malware analysis system. It is estimated that around 75 Gbps have improved the DDoS attack mitigation capability of AIS with the DDoS attack mitigation system already provided and installed. The malware analysis equipment is not yet operational.

Therefore, the output 2-2 “*Reactive infrastructure is improved*” is partially achieved.

Output 3-2: Proactive infrastructure is improved

The equipment that improves Proactive service is the DDoS attack mitigation system and Evaluation lab equipment. The DDoS attack mitigation system is now in operation, but the security evaluation equipment has not yet been put into operation.

Therefore, the output 3-2 “*Proactive infrastructure is improved*” is partially achieved.

2-2 Project Purpose and indicators

<Past information>

The project team checks the achievement status of the project purpose, “Capacity of AIS for cybersecurity is enhanced”, from the following two indicators.

Indicator		Means of Verification
1	AIS assigns the appropriate roles to each staff to optimize organizational performance.	List of organizational structure with staff roles
2	Each AIS staff fulfills the assigned roles.	Staff evaluation based on career development plan (CDP)

For indicator 1 of the Project Purpose, the project team has assigned SecBoK roles to each staff.

For indicator 2, based on the CDP review, there were many examples of staff assigned to various roles improving their daily work and changing their mindset through training using CDP methods. Quantitatively, an increase in scores has been observed by comparing post-test scores and online learning scores with the pre-test scores. In addition, there has been a steady increase in the number of trainees taking and passing certification exams. From these results, it can be concluded that the capacity to fulfill the assigned roles is steadily improving.

Through the activities of awareness raising, the staff in charge of the COP has learned how to consider the contents for the awareness materials and how to coordinate with video production companies. The ability to analyze larger dissemination strategies and target groups can be learned in the upcoming awareness raising seminar. Thus, the goals of improving individual capacity through training and awareness raising are being achieved.

On the other hand, there are risks involved in providing equipment to achieve the goal of acquiring reliable configuration and operational capabilities. The provision of two types of equipment has been delayed, leaving insufficient time for installation and transition to operation.

Therefore, it can be concluded that the project purpose is not yet achieved but the project is making steady progress toward achieving the project purpose.

(1) Effectiveness and efficiency of Training

Staff who took the training and their supervisors were asked whether they felt that the training was effective in their daily work after taking the course. Supervisors were asked to respond to each trainee who took the training. About 80% of the participants answered that they and their supervisors felt that the training was effective. However, there was little information on the specific situations in which the training was effective. The reasons for this are as follows. The training courses we have provided so far cover very basic topics such as CompTIA Security+, ECSS, Linux, etc. So, even if they felt the training was practical, it would be difficult to explain the effective situations in. When training directly related to business operations is implemented in the future, it is expected that more concrete results can be confirmed.

In conclusion, the complementary quantitative indicators and the results of the CDP review indicate that the effectiveness is medium level.

(2) Effectiveness of CDP

Eight superiors indicated that the CDP was effective among 14. The remaining six responded that the CDP was effective but needed to be improved. See the next section for more information on improvement requests and project actions.

Question				
What do you think of CDP? Is it useful for your organization and your management? Please select one from the list and describe the reason why you selected it.				
Useful	Useful but need improvement	Not useful must be changed	Not useful at all	Total
8	6	0	0	14

* The reason the total is 14 is due to the reason as mentioned earlier.

(3) Improvement of Training and CDP

The following table summarizes the main requests for training and CDPs obtained from staff and division heads, and the project's response to them.

Table 7 Comments for CDP and training and its improvement

No	Comments or Opinions	Action
1	SecBoK Roles: Security roles of the SecBoK are difficult to understand. It is difficult to understand the correspondence between SecBoK Roles and actual roles in VNCERT/CC. If there is a kind of table that shows the relationship, it may be helpful.	The correspondence between SecBoK roles and NIST roles already exists. However, understanding and applying Role is difficult. Currently, we do not use SecBoK's mapping directly, but rather assign courses based on the job description and the person's needs through interviews. Once the Vietnam Security Role Standards are finalized, we may create a correspondence between them and the NIST roles. We will also clarify the courses that each Role should take in the future.
2	Balance between work load and training: The week of training was too busy so that I participated in the training by separating the training from my daily work. For some supervisors, training is less of priority than for other duties.	CDPs are shared with superiors at the time of new creation and review to ensure that they are reviewed and agreed to participate in training. Since training is a high priority in AIS's work, make sure the superiors understand its importance and encourage them to make sure their subordinates are involved in the training. Share the briefing paper created by the project to help them understand it.
3	Training term: The training term was too short so he could not learn all of the contents. 5 days course full time training may not be so effective since the course contents are too much to teach everything during 5 days.	It is difficult to take more than 5 days for the one course. The training will give trainees an outline of the whole contents, and then trainees can consolidate your knowledge by learning on your own for 1-3 months at a prepared learning website (Preparation for examination).
4	Additional training for the exam: Additional class for the exams was useful. Hope more practical training.	Since the purpose of the training is to learn concepts and the overall picture, and not to prepare for exams, there will be no additional classes for examination preparation.
5	More practical training: There was only a demo and not a lot of hands-on time. Hope more practical training.	Custom training that includes a lot of hands-on such as CSIRT and malware analysis will also be prepared in the future. Other custom training will also be designed to incorporate needs in advance so that they can be directly useful to the security business.
6	English barrier: English is challenge for the course.	We are planning to provide the technical English course.
7	Training participants: Expand the scope of the training to MIC staff other than AIS and government officials other than MICs.	The priority for the training target is the project counterpart, AIS. To provide training systematically, it is assumed that the target people would have a CDP prepared. During the preparation stage of the training, it is possible to involve participants from outside the AIS if it is possible to increase the number of training slots at no additional cost (government officials other than the Ministry of Defense or the military). However, as with AIS, it is difficult to plan and involve them from the outset due to the following reasons: - Due to the limited budget and timeframe, coordinating other government officials as the target participants from the beginning would reduce the opportunities for AIS staff to participate in the training. Currently, there are 80 participants, but as the number of AIS staff increases, the project will include as many staff who wish to be trained as possible. - If one department other than AIS is scheduled to participate in the training, other departments will also ask to join. If we prioritize a particular department, it would be unfair, and an undesirable atmosphere might be created for the project.

3. History of PDM Modification

The PDM was changed in the 2nd JCC (14th August 2021). The reason for the change is described in the Minutes of Meeting dated 27th August 2021. The Minutes of Meeting and PDM of the JCC are attached to this report as Appendix.

4. Others

4-1 Results of Environmental and Social Considerations

No consideration due to the category C[2], which means that the project is likely to have a minimal or little adverse impact on the environment and society.

4-2 Results of Considerations on Gender/Peace Building/Poverty Reduction

No consideration on Gender, Peace Building or Poverty Reduction for the Project.

III. Results of Joint Review

1. Results of Review based on DAC Evaluation Criteria

1-1 Relevance

1.1.1 Vietnamese Development Policy and Plan

As of the start of the project, Viet Nam enacted the National IT Law in 2007, which stipulates the rights and responsibilities of the government, organizations, and individuals in the development and use of IT technologies, as well as decrees and ministerial ordinances to ensure the information security on the Internet. In 2010, the penal code on Information Security was amended to stipulate specific details and penalties for DDoS attacks, intentional spread of computer viruses, and online fraud, and the government is focusing on information security measures.

National strategies and cybersecurity plans have also been enacted, such as Prime Minister's Decision No. 63 of 2010 “Approval of the National Plan on the Development of Digital Information Security until 2020” and Prime Minister's Decision No. 898 of 2016 “Direction, Goals and Objectives for Ensuring Cyber Information Security from 2016 to 2020”. Decision of the Prime Minister No. 898 of 2016 “Approval of the Direction, Goals and Obligations to Ensure Cyber Information Security from 2016 to 2020” stipulates various goals, plans and organizational structures of cyber security to be achieved by 2020 as the Government of Viet Nam. Prime Minister's Decision No. 893 of 2015 “Approving the Project on Propagation, Dissemination and Enhancement of Awareness and Responsibility for Information Security by 2020” stipulates targets and publicity activities on communication, dissemination and promotion of cyber security by 2020. The Prime Minister's Decision No. 99 of 2014 “Approving the Scheme on Human Resources Training and Development on Information

[2] https://www.jica.go.jp/english/our_work/social_environmental/index.html

Safety and Security" stipulates targets and plans for human resources development in the field of cyber information security until 2020.

In 2018, the Law on Cyber Security was enacted, which has features that stipulate, among other things, ensuring a mechanism to guarantee the identity of users when developing online services in Viet Nam and providing and deleting data to competent authorities upon request.

As of the end of the project, the Prime Minister's Decision No. 749 of 2020, "National Digital Transformation Program by 2025," includes "developing a digital society and bridging the digital divide" as one of its objectives. It also aims to be ranked in the top 40 by the Global Cyber Security Index (GCI) published by the International Telecommunication Union by 2025 and in the top 30 by 2030 (Vietnam is ranked 25th in the GCI in 2020). It also sees cybersecurity as the key to successful digital transformation and a sustainable society. To focus on security education for young people, particularly vulnerable among general users, the Prime Minister's Decision No. 830 on "Project for Protecting and Supporting Youth to Use Cyberspace Creatively and Safely (2020-2025)" was issued in June 2021. Based on this decision, Viet Nam is promoting awareness-raising activities on cyber security and information security, especially for youth. (Other latest policies will be added when the report is finalized.)

Therefore, this project is consistent with the policies of the Vietnamese government at the time of planning and at the time of completion of this project.

1.1.2 Development Needs

Before implementing this project, the number of incidents in Viet Nam had been increasing rapidly since 2014, and in 2015, the number of confirmed incidents of phishing attacks, website tampering, malware, etc. exceeded 30,000 (compared to about 6,000 in 2013). In 2016, there were more than 120,000 confirmed cases of the same attacks. In the same year, Viet Nam Airlines' website, voice system, and electronic board related to flight information were hacked, resulting in the airline's customer information leakage. Later in 2019, the number of cyberattacks of the above three types was around 5,000. Note that the method of surveying cyber-attack methods and the number of incidents may differ from year to year, and the quality of cyber-attacks may differ, so a simple comparison of the number of incidents should be made with caution.

It has become clear that the information systems of government agencies and organizations have many vulnerabilities and pose a significant cyber security risk. In addition to the above three types of incidents, external intrusions, DoS/DDoS attacks, and APT attacks (Advanced Persistent Threats) have increased. In addition, malware infections are increasing every year, especially through social networks. Online phishing is also still prevalent, and many users are suffering financial losses due to overconfidence and carelessness in information security. Furthermore, there have been many DDoS attacks with mass attacks targeting IoT devices such as routers and security cameras, causing damage and impact on the operation of many communication services. Personal information leakage is also significant, and the number of incidents causing economic losses to users in banking, finance, and e-commerce is increasing.

At the end of this project, in addition to the previous cyberattacks, the threats related to cyber-security have continued to increase, such as more than 50% of small and medium-sized enterprises (SMEs) in Viet Nam were aware of cyberattacks, and cyberattacks targeting important national organizations, youth and children have been increasing.

In Viet Nam's information and cybersecurity system, the Ministry of Defense (MOD) and the Ministry of Public Security (MPS) are in charge of cyber defense and cybercrime investigation, respectively. The AIS under the MIC), which is the counterpart of this project, formulates the national cybersecurity strategy and has a Security Operation Center (SOC) and a Computer Incident Response Team (CERT) that specializes in security issues. Although the AIS has been able to conduct awareness-raising activities, incident response, and cyberattack prevention to a certain extent, it is important to further enhance the capabilities of security engineers in order to strengthen the government's network monitoring, cyberattack prevention, and incident response functions against the ever-increasing and sophisticated cyberattacks.

At the beginning of this project, there was a separate organization within the MIC, the Viet Nam Computer Emergency Response Team (VNCERT), which was established earlier than the AIS and had the same SOC and CSIRT as the AIS. However, the difference was that AIS had a policy formulation function and a DDoS attack mitigation system, while VNCERT/CC had a control function among related organizations to support the establishment of CSIRTs in other organizations. VNCERT was incorporated into the AIS as VNCERT Coordination Center (VNCERT/CC) in November 2019 after the project started.

Five government agencies provide security support to operators (including central and local government agencies) of critical information infrastructure for power and transportation, etc., including VNCERT/CC and AIS (National Cyber Security Center (NCSC)) (the others are located within the MOD and the MPS). Each has functions similar to SOC, CSIRT, and Japan's Cyber Incident Mobile Assistant Team (CYMAT). Operators can request assistance from any of the above five agencies, and in some cases, one operator will have monitoring sensors from both VNCERT/CC and AIS.

To ensure redundancy of defense against cyberattacks (i.e., even if one defense system is breached, other systems can still provide protection), the establishment and enhancement of multiple SOCs and CSIRTs are supported. In particular, supporting AIS that has cyberattack mitigation systems and also formulating cyber security policies is important to strengthen the cyber security system of the entire Vietnamese government.

Therefore, it can be said that there is a high need for development on cyber security at the time of planning and at the end of this project.

1.1.3 Consistency with Japan's aid policy

Japan's “Development Cooperation Charter” (February 2015) lists “strengthening the capacity of developing countries in international public goods such as maritime, outer space, and cyber space” as a policy of its priority issue “sharing universal values and realizing a peaceful and secure society,” which is consistent with the purpose of this project.

At the time of the start of the project, the “Cyber Security Strategy” approved by the Cabinet in July 2018 states that Japan will work to ensure cyber security through international cooperation with various entities to realize peace and stability of the international community and Japan's security. The “Policy for International Cooperation on Cyber Security” in October 2013 states that Japan will strengthen cooperation such as capacity building and knowledge sharing with the Asia-Pacific region, especially ASEAN countries, which have the closest geographical proximity and economic relationship with Japan. Furthermore, the “G7 Principles and Actions on Cyber” agreed at the G7 Ise-Shima Summit (2016) also states the policy to enhance cyber security by supporting international cooperation, capacity building, awareness-raising, and support among CSIRTs. In addition, Viet Nam requested Japan's cooperation in the cyber field at the Japan-Viet Nam Summit Meeting in January 2017.

At the end of the project, the “Cyber Security Strategy” approved by the Cabinet on September 28, 2021 states that Japan will continue to promote knowledge sharing, policy coordination, international cooperation on cyber incidents, and support for capacity building, as it is important to cooperate and collaborate at various levels, including governments and private sectors, since cyber incidents in other countries may easily affect Japan.

This project is positioned as one of the priority areas “(3) Strengthening Governance” in the Ministry of Foreign Affairs' “Policy on Development Cooperation with the Socialist Republic of Viet Nam” (December 2017 and 2012). In addition, the enhancement of cyber security will contribute to “(1) Enhancing Growth and Competitiveness” by realizing stable ICT infrastructure operation.

At the beginning of the project, the “JICA Country Analysis Paper to Viet Nam” (March 2014) listed the enhancement of judicial and administrative functions to strengthen governance as an important development issue. In the latest JICA Country Analysis Paper to Viet Nam (June 2020), strengthening governance (improving governance capacity) was also listed as a priority area at the end of the project. In particular, concerning the enhancement of legal enforcement capacity, it is necessary to develop human resources and appropriate law enforcement to improve cyber security capacity.

Therefore, it can be said that the project was consistent with Japan's policy at the time of planning and completion.

Based on the above, it is concluded that the implementation of the project is highly appropriate as it is fully in line with Viet Nam's development policy, development needs and Japan's aid policy. Therefore, its relevance is high.

1-2 Efficiency

1.2.1 Input

Input	Plan (as of Project start)	Actual (as of Project completion)
Japanese side		
Total amount of cooperation	153 million JPY	319 million JPY
Project term	June, 2019 - November, 2021 (30 months)	June, 2019 - June, 2022 (37 months)
Dispatch of experts	Dispatched: 2 Remote support: 1	Dispatched: 2 Remote support: 4
Trainees in Japan (including online courses)	-	14
Trainees in Viet Nam	40	106 (Final count) 144 (Cumulative count)
Trainees in third country	-	2
Equipment	45 million JPY (DDoS mitigation, network monitoring, malware analysis, etc.)	78 million JPY (DDoS mitigation, network monitoring, malware analysis, evaluation lab etc.)
Local operation cost	44 million JPY (local training, local procurement, project staff, etc.)	128 million JPY (local training, local procurement, project staff, etc.)
Vietnamese side		
Counterpart staff	3	6
Facilities	Project office, internet, electricity, etc.	Project office, internet, water supply, electricity, etc.

1.2.2 Input components

There were some problems with the input items of this project.

First of all, regarding the input of the Japanese side, initially, the JICA experts were long-term experts and short-term experts (chief advisor and career development plan), but in response to the needs of the Vietnamese side, the experts in Awareness-raising activities and ISAC, etc. were added. Training by the relevant organizations in Japan and on-site training was also conducted at generally appropriate times in the context of COVID-19, making full use of the online video conferencing system. One year after the start of the project, several pieces of equipment were added at the 1st JCC, but most of them were delivered before the end of the project. Furthermore, it turned out that some of them would be delivered after the end of the project, so the project had to be extended for the second time.

There were no major problems with the Vietnamese inputs. Three months before the end of the project (in December 2021), the Deputy Project Director (DDG of AIS), who was in charge of coordination on the Vietnamese side, was moved to another position. After that, there was no opportunity to coordinate with the Project Director (DG of AIS) at meetings, etc., but this did not pose a major problem because the necessary coordination was almost complete, and the activities were nearing completion.

1.2.2 Amount of Cooperation

The amount of cooperation was planned to be 153 million yen, but it turned out to be 319 million yen (208% of the plan), far exceeding the initial plan.

1.2.3 Cooperation Period

The period of cooperation was planned to be 30 months, but it turned out to be 37 months (123% of the plan), far exceeding the initial plan.

As described above, although the amount and duration of the cooperation increased significantly, there is no problem because only the inputs necessary to achieve the project purpose were added, and the changes were decided following an appropriate process.

On the other hand, the timing of the provision of most of the equipment was concentrated in the latter half of the project, which did not contribute sufficiently to the realization of the project effects, and thus the efficiency of the project was judged to be somewhat low.

1-3 Effectiveness

1.3.1 Outputs

(1) Capacity of security quality management and policy making is enhanced

Indicator 1-1: CDPs are set.

Through interviews with a short-term expert, Career Development Plans for each AIS staff member were prepared and updated at the time of CDP reviews. The total number of CDPs prepared was 144, and the number of CDPs at the end of the project was 106. (The decrease is due to resignations and moving after the creation.)

Indicator 1-2: Capacity of the trainees is improved.

Following the career development plan for each staff member, training on security technology, project management, business English related to cyber security, etc. were generally implemented as planned. The results of the knowledge verification test conducted before and after the training showed that most of the trainees improved their knowledge before and after the training. In the online self-study in the months following the intensive training, it was confirmed that almost all of the trainees who engaged in the practice improved their technical knowledge significantly from before the training. In addition, for certification-related training only, the performance on the international certification examinations taken by trainees who had reached a certain level of online learning also improved from the pre-training level, with about 50% of the trainees related to the certification examinations passing (or about 80% if the number of successful candidates is limited to the number of candidates). In the CDP review, there were many cases in which the knowledge gained in the training was utilized in work, and many trainees were motivated to learn more after passing the certification.

As described above, there were both quantitative and qualitative signs of improvement in the trainees' security skills at the end of the project.

Indicator 1-3: Number of awareness materials is increased.

Through this project, we have developed animated videos (3) on cyber security for youth and children, a design kit familiar to the public, and a portal site with functions such as information disclosure and reporting of illegal contents from the public.

Indicator 1-4: The developed materials are used.

The animation videos developed have already been made available on the AIS Youtube channel. One of the videos, “Introduction an Online Contest of Information Security for students,” was shown to introduce the contest at VIETNAM INFORMATION SECURITY DAY 2021 (held on November 25, 2021), which the Minister of MIC attended. It is expected that the design kit will be actively used in future promotional activities to promote the public's awareness of cyber security. The portal site is expected to be used as a tool for the citizens to communicate with the government side as well as to disclose necessary information for the citizens as the AIS continues its operation.

Indicator 1-5: Acquired knowledge for practice of policy making is utilized (Based on the interview survey with AIS)

In the CDP interviews with the trainees who took the training on policy formulation, many of them said that the Japanese policies (especially product security inspection, information sharing system, support for SMEs, etc.) and GDPR initiatives were beneficial for their work. However, by the end of the project, we could not confirm any concrete examples of the implementation of the policy-related training into Viet Nam's policies.

As a result, Indicators 1-1, 1-2, and 1-3 were sufficiently achieved, while Indicators 1-4 and 1-5 need to be continued to be utilized in order to achieve the effect. Therefore, it can be concluded that Output 1 was generally achieved.

(2) Capacity of reactive service is enhanced

Indicator 2-1: Capacity of the trainees is improved.

See Indicator 1-2.

Indicator 2-2: Reactive infrastructure is improved (Judged from the report from AIS)

The DDoS attack mitigation system was delivered in March 2021 and was confirmed to have been installed and in operation in November 2021. Training on Linux OS and virtual machine (VMWare) was conducted as technology for direct operation during the project. The malware analysis system has not been delivered as of the end of February 2022 and will be delivered just before the end of the project. Training for analysis methods and advice on operations were provided with JPCERT/CC.

As a result, Indicator 2-1 has been achieved satisfactorily, but the effect of the project activities has not been fully realized for Indicator 2-2, which requires continuous operation by the AIS. Therefore, it is judged that Output 2 has been generally achieved.

(3) Capacity of proactive service is enhanced

Indicator 3-1: Capacity of the trainees is improved.

See Indicator 1-2.

Indicator 3-2: Proactive infrastructure is improved

See Indicator 2-2 for DDoS attack mitigation system.

The evaluation equipment related to the Common Criteria has not been delivered as of the end of February 2022 and is scheduled to be delivered just before the end of the project. As for the evaluation equipment's security measures and operational procedures, a local company provided consulting services to prepare the necessary documents and procedures and conducted technology transfer through training.

As described above, Indicator 3-1 was fully achieved, but the effect of the project activities on Indicator 3-2 has not yet been fully realized. Therefore, it is judged that Output 3 has been generally achieved.

1.3.2 Project Purpose

- **Project Purpose: Capacity of AIS for cyber security is enhanced.**

Indicator 1: AIS assigns the appropriate roles to each staff to optimize organizational performance.

Indicator 2: Each AIS staff fulfils the assigned roles.

From the above, it is judged that each of the three outputs has been “generally achieved”. In addition, it is difficult to judge that indicators 1 and 2 of the project purpose have been fully achieved, although some of them have been achieved. Therefore, the effectiveness of the project is judged to be moderate.

1-4 Impact

1.4.1 Achievement of overall goal of the project

- **Overall goal of the project: Cyber resilience for Vietnamese government is increased.**

  Indicator: AIS contributes to achievement of the objectives in the cyber security policies (e.g. Decision No.63/2010, No.898/2016 and No.893/2015) by 2020. *Targeted policies will be confirmed after the Project starts.

  The evaluation policy was to measure the contribution of the project to the overall objectives by assessing the contribution of AIS in achieving the policy objectives based on interviews with AIS, Annual Reports, and statistical information published by AIS. However, AIS has not published Annual Reports have not been issued. Therefore, we will use interviews with staff, including CDP reviews, to infer the emergence and likelihood of effectiveness of the overall goal.

  The overall goal, cyber resilience, refers to the mechanisms and capabilities to minimize the impact of cyberattacks on systems and organizations and quickly restore them to their original state. In other words, cyber resilience is the ability to respond to a cyberattack that may shut down critical information infrastructure or suspend government operations to continue government administration and operations. Among the five functions of cyber security in NIST's Cybersecurity Framework Version 1.1[3], namely “Identify,” “Protect,” “Detect,” “Respond,” and “Recover,” the three functions of “Detect,” “Respond,” and “Recover,” are the components of resilience. After “Identify” threats, attackers, and vulnerabilities using threat intelligence and “Protect” the system with security measures, it is necessary to enhance the capabilities of “Detect,” “Respond,” and “Recover” in parallel, assuming damage and intrusion. The key points of cyber resilience are the formulation of security policies and guidelines, establishing security measures, monitoring network traffic to understand the situation, and establishing a detection and response system in case of cyber incidents.

  To strengthen these systems and capabilities, the project's outcome was to enhance the three service capabilities (security quality management services, proactive services, and reactive services) as defined by the European Union Cyber Security Agency (ENISA). By improving the capabilities of AIS human resources and equipment, the project strengthens AIS's ability to develop, monitor, and respond to policies and guidelines, thereby improving AIS's cyber resilience. It is reasoned that enhancing activities such as Information Sharing and Analysis Center (ISAC), Common Criteria

[3] https://www.nist.gov/cyberframework/framework

security evaluation and certification, and COP, which were also supported by the project, will contribute to strengthening the resilience of Viet Nam as a whole by enhancing cooperation among government agencies, local governments, and the private sector. In the Global Cybersecurity Index (GCI), which assesses the maturity of cybersecurity in terms of systems, technology, organization, capacity building, and cooperation, Viet Nam's cybersecurity is ranked 25th in 2020 (50th in 2019 and 101st in 2017). relatively strengthened.

Therefore, if the AIS continues its mission to maintain the same level of progress as during the project period and to continue and strengthen its effectiveness after the project ends, the impact is likely to become apparent several years after the project ends.

1.4.2 Other impact

(1) Impact on the natural environment

PCs, servers, and other devices were only installed in the existing facilities, so there was no negative impact on the natural environment.

(2) Residents and land acquisition

PCs, servers, and other devices were only installed in the existing facilities, so no resettlement or land acquisition has occurred.

(3) Other indirect effects

None in particular.

From the above, it can be judged that the project is making steady progress toward achieving the overall goal expected from the implementation of the project, although it cannot be said that sufficient impact has been realized.

1-5 Sustainability

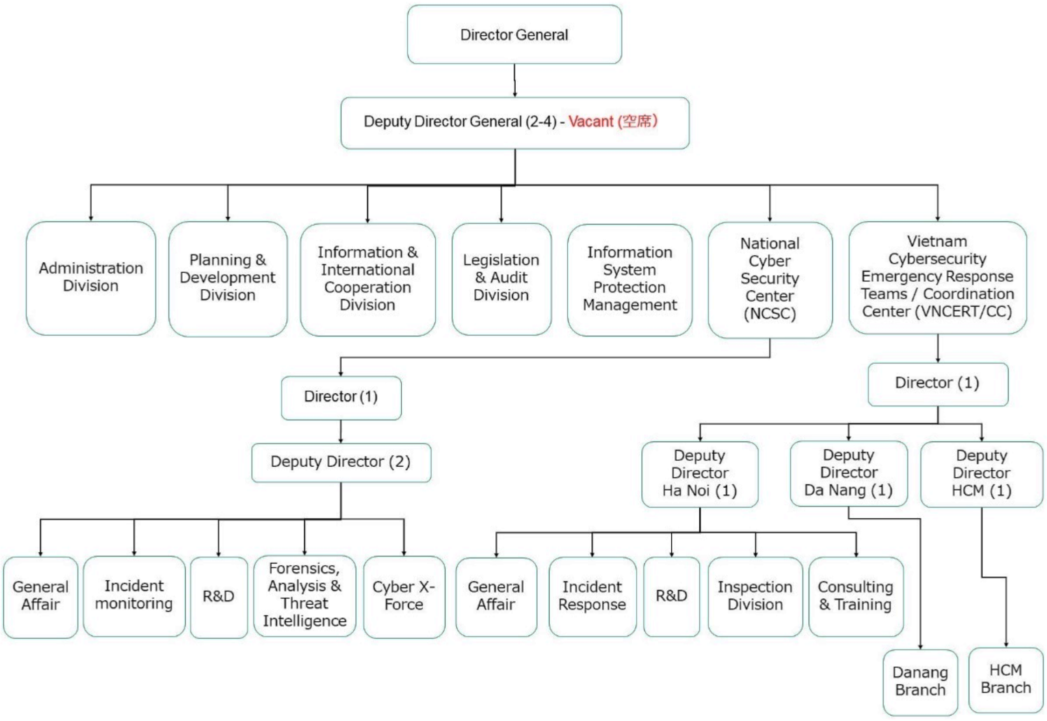
1.5.1 Policy and Political Commitment for the Sustainability

In the Prime Minister's Decision No. 749 of 2020, “National Digital Transformation Program by 2025,” cybersecurity is seen as a key to successful digital transformation and making society sustainable. Based on the Prime Minister's Decision (No. 830) of June 2021, “Project to Protect and Support Youth to Use Cyberspace Creatively and Safely (2020-2025),” the government is promoting public awareness activities on cyber security and information security, especially for vulnerable youth and young adults. There is no change in AIS's role during these strategies.

Therefore, it is judged that sustainability in policies and systems is high.

1.5.2 Institutional/Organizational Aspects of the Sustainability

AIS has been undergoing minor organizational changes to improve operational efficiency since the merging of VNCERT/CC in November 2020. The organizational structure of the AIS as of February 2022 is as follows



Director General
Deputy Director General (2-4) - Vacant (空席)
Administration Division
Planning & Development Division
Information & International Cooperation Division
Legislation & Audit Division
Information System Protection Management
National Cyber Security Center (NCSC)
Vietnam Cybersecurity Emergency Response Teams / Coordination Center (VNCERT/CC)
Director (1)
Deputy Director (2)
General Affair
Incident monitoring
R&D
Forensics, Analysis & Threat Intelligence
Cyber X-Force
Director (1)
Deputy Director Ha Noi (1)
Deputy Director Da Nang (1)
Deputy Director HCM (1)
General Affair
Incident Response
R&D
Inspection Division
Consulting & Training
Danang Branch
HCM Branch

Da Nang City and Ho Chi Minh City, where VNCERT/CC branch offices are located, lack resources, but efforts are being made to actively recruit human resources in each department, including these branch offices. As of February 2022, there were no AIS Deputy Directors, compared to four at the start of the project, making the operational management system vulnerable. However, it is judged that there will be no problem with the management system once the two planned Deputy Directors take office around March 2022.

1.5.3 Technical Aspects of the Sustainability

Although there is always the risk of transfers and retirements, as long as the personnel trained by this project continue their work, there will be no significant problems with technology. When it comes to IT and cyber security, learning a skill once is not the end of the world, but it is necessary to learn new skills constantly. The MIC has a budget for regular training, and if the staff understands the importance of career development through this project, they should be able to learn a certain amount of new knowledge from any training. The skills and knowledge transferred through this project have been accumulated in the form of training materials and manuals, and if these are used as on-the-job training, the skills can be sufficiently passed on. Continuing to recruit new human resources, AIS continues to retain staff with university-level knowledge and motivation, and it is expected that a certain number of skilled personnel

will be retained in an industry where transfers to other workplaces are frequent. With regard to the provided equipment, no significant problems are expected since similar equipment has been operated and maintained in the past.
Based on the above, it is judged that there are no problems with the technology.

1.5.4 Financial Aspects of the Sustainability

Detailed information on MIC's finances is not available. However, it is reported that government project budgets for COP, CC evaluation and certification system, and establishment of ISAC, which are issues that AIS should continue to work on, have been secured from 2022.

As a result of the above, there is no detailed information on the finances after completing the project. In addition, due to minor issues with the counterpart's organization, the sustainability of the effects of the project is moderate.

2. Key Factors Affecting Implementation and Outcomes

The risks that were managed from the beginning to the end of the project and how they were addressed are listed below. Note that [ ] indicates the version of the Monitoring Sheet at the time of the response.

Risk	Impact Level[4]	Status and Measurement
1. Equipment tax exemption issues	Efficiency Low	[MS1] Soon after starting the project in June 2019, the Ministry of Foreign Affairs and Ministry of Finance have not issued the Aid Certification required for the tax exemption procedure. In some cases, the Vietnamese project executing agency could not complete the tax exemption procedure for the provided equipment. [PCR] The tax exemption issue has been resolved in November 2019.
2. SecBoK role and skill mapping issues	Efficiency Effectiveness Low	[MS1] SecBoK role definition and technology mapping to the roles are ambiguous or incorrect for some cases. If no significant problem occurs, use the SecBoK roles and mapping as they are. If a problem does occur, we adjust the mapping in the project independently. [PCR] Created and incorporated into the manual as a deliverable for the Career Development Plan in February 2022.
3. Training mapping to SecBoK	Efficiency Effectiveness Low	[MS1] Not implemented. We will map it at the timing of the next CDP review.
4. Absence of training	Efficiency Effectiveness Medium	[MS1] Some trainees have missed some classes in CompTIA Security+, CEH that have been conducted to date. Some trainees would not attend the class because they only wanted to take the CEH certification. Trainees must understand that the purpose of the training is to improve their practical skills in the business, rather than to gain certifications. [MS2] Some trainees have missed some classes in CompTIA Security+, CEH, and CCNA Security that have been conducted to date. Some trainees would not attend the class because they only wanted to take the CEH certification, and some had abandoned the course at CCNA Security. As a countermeasure, from ECSS courses, the project team confirms the trainee's intention to take the course. At the start of the lecture, we re-announce that trainees can take the certification exam if they attend by all classes, and if it is unavoidable to be absent, they must notify JICA in advance. Trainees must understand that the purpose of the training is to improve their practical skills in the business, rather than to gain certifications.

[4] low, medium, high, and very high

Risk	Impact Level[4]	Status and Measurement
5. Taking the certification exam	Efficiency Effectiveness Medium	[MS1] The purpose of taking a certification exam after the training is to measure the training results. The following conditions will be applied to increase the pass rate of the certification exam. (will applied from the 3rd training) 1. Attend all classes (other than absences for reasonable cause). 2. A pass rate of 90% or more in the mock test conducted one month after the training. The project will provide funding if the test passes, and the CP will pay if it fails. Because the purpose of taking the certification exam is to measure the outcome of the training, we will consider it in the future so that the first exam will be possible for all trainees. [PCR] Finally, it was decided that students who meet the following requirements in the online mock exam would be allowed to take the certification exam only once. 1. Attempt at least 10 times (This does not apply if trainee have studied by books, etc.) 2. The average score of the last three attempts must be 90% or higher, OR 90% or higher for two consecutive attempts.
6. Delay in equipment procurement	Efficiency Effectiveness Medium	[MS1] Approval process of Project Document is taking a long time. This process is difficult to control due to the involvement of various ministries in Viet Nam. We will also work on AIS and procure equipment by 2020. [MS2] Approval process of Project Document was approved on 3 June 2020. Now we will also work on AIS and procure equipment by 2020. [PCR] Delivery completed in March 2021.
7. Delay in the development of educational materials	Efficiency Effectiveness Medium	[MS1] We spent much time (eight months) after the start of the project for coordinating with the awareness-raising staff and could not develop educational materials yet. Since we agreed on the direction of our activities in March 2020, we will resume preparing educational materials after April 2020. [MS2] We started the procurement process for the 1st video clip. [PCR]. Three animation videos were created by the end of the project.

Risk	Impact Level[4]	Status and Measurement
8. Ensuring sustainability after project completion	Sustainability Medium	[MS1] The policies and initiatives of the Vietnamese side regarding sustainability among the five Development Assistance Committee (DAC) evaluation items (whether the benefits of the project will be sustained in terms of policy, technology, organization, and finances). - As of January 2020, AIS was considering a classification for the role of government security officials and the required technical areas. Although it is a different classification from SecBoK and NICE Framework, creating a mapping with them may be useful for efficient training plans and human resource development in the future. The project team will develop a guideline which instructs how to create and manage the CDP in the future, so that they can be used after the end of the project. - There is always the risk that staff with technical skills will change jobs. However, it is difficult to control them from the project. It may lead to a slight improvement, for example, to give qualified staff some incentive from AIS. - About awareness raising activities, cybersecurity is a rapidly changing field. In contrast, password strengthening or countermeasure against phishing attacks will continue to be important for some time. After we develop educational materials, they are expected to be used continuously. - It is expected that the equipment will be used continuously by performing necessary maintenance. Still, IT equipment will need to be updated at the required timing as its specifications improve year by year.
9. Limits of courses that can be held in Viet Nam	Efficiency Effectiveness Medium	[MS2] The following planned courses are challenging to implement due to location (overseas) or cost. SEC542 : Web App Penetration Testing and Ethical Hacking, SEC511: Continuous Monitoring and Security Operations, FOR508: Advanced Digital Forensics, Incident Response, and Threat Hunting, FOR578 : Cyber Threat Intelligence, SEC560 : Network Penetration Testing and Ethical Hacking" FOR610 : Reverse-Engineering Malware: Malware Analysis Tools and Techniques
10. Taking online practice and certification exam Related to No. 5 risk	Efficiency Effectiveness Medium	[MS3] Status: In the past six months, the period covered by the report, very few people took online learning or certification exams. When asked the reasons in the 2nd CDP review, the following reasons were given. 1. In the project management certification training (CAPM and PMP), it was found that the trainees felt the international standard project management methods were not suitable for management in Viet Nam. (Therefore, the motivation to learn was not maintained.) 2. The trainees were busy with work towards the end of the year. Countermeasure: • In the project management training, it was recommended that the participants understand the following and learn online as much as possible ○ Not all of the contents need to be applied to work in Viet Nam. ○ Try to incorporate those contents that are partially applicable, such as scheduling and human resource management.

Risk	Impact Level[4]	Status and Measurement
		o International standard management methods may be helpful when working with overseas stakeholders. • For training conducted by November 2020, the online learning period will be extended to March 2021, and it will be allowed to take the certification exam if the conditions are met. • In the future, the online learning period after intensive training will be extended to about three months or more. Monitoring of online learning status will be strengthened, and frequent e-mails will be sent to encourage learning and taking the certification exam.
11. Delay in approving Project Document and Signing updated R/D Related to No. 6 risk	Efficiency Effectiveness High	[MS3] Status: • With respect to the extension of the project period decided at the 2nd JCC in August 2020, it may take some time to approve the updated Project Document and sign the updated R/D. • The following will have a significant impact on project activities, as they can only be procured after approval and signature. o Malware analysis equipment o Evaluation lab equipment o ISAC expert o Awareness raising experts Countermeasure: • Monitor the status of each process frequently and proceed with the process with the cooperation of AIS executives and JICA Viet Nam Office. • Finalize the content of the updated R/D ahead of schedule and be ready to sign it immediately after the approval of the updated Project Document. Prepare for the procurement of additional equipment and experts ahead of schedule so that the process can proceed immediately after the approval and signature.
12. Delays in delivery of malware analysis and evaluation lab equipment	Efficiency Effectiveness High	[MS4] Status: About the evaluation lab, which was decided to be added by the 2nd JCC in August 2020, and the malware analysis equipment that was included in the component from the beginning, there were several requests from AIS for additional equipment. Then the specification decision took until January 2021. Since then, the project document approval process within the Vietnamese government has taken some time, and as of June 30, 2021, the approval has not been completed. After the approval is given in July, it is assumed that it will take another month or so for the signature process of the updated RD. Therefore, procurement of equipment will start around the end of July 2021, and delivery will be around the end of September or October 2021 at the earliest. January to March 2022 is the project summary period, and even if this period is used as buffer time, the equipment should be set up and operational by December 2021. The following measures are being taken to ensure a smooth and efficient equipment procurement and setup

Risk	Impact	Status and Measurement
	Level[4]	
		process after the project document is approved.
		Countermeasure: • Preliminary preparation of RD: Preliminary confirmation of AIS and preliminary confirmation at JICA headquarters have been completed. • Preparation of equipment estimate: The latest versions were obtained at the end of April 2021, but they were expired in June 2021, so the latest version will be obtained in July 2021. • Sufficient advance preparation for setup: As part of the preparation for acceptance, AIS needs to secure the installation site and confirm the network settings. in advance. • Operational support: Local companies will be requested to create operational policies and procedures regarding malware analysis equipment and evaluation labs. JPCERT/CC will also provide advice on malware analysis equipment. [MS5] Status: It is more likely that some of the Malware analysis system and Lab equipment will be delivered later than the project end date (March 2022). Countermeasure: The project and JICA are considering extending the project for a few months to allow for delivery after April 2022. However, all activities other than the receipt of equipment will be completed at the end of March 2022.
13. COVID-19	Efficiency Effectiveness	[MS4] Since May 2021, the situation of COVID-19 has worsened throughout Viet Nam. Trainees residing in Da Nang or HCMC will be allowed to participate in the training online depending on the situation. If the instructor resides in HCMC, the training itself will be conducted online. [MS5] From the second half of 2021, the Vietnamese government is taking a stance to promote vaccination and acceptance of COVID-19, without taking strict measures such as lockdown. The project will continue its activities with due care and attention in accordance with the government's infection control measures.
	High	
14. Delay of Phase 2 request	-	[MS4] For the components envisioned in Phase 2 project, the current project has provided some support in terms of capacity building of staff. In order to maximize the effectiveness of the projects, it is recommended that the phase 2 project be implemented no later than the end of the current project. Since the deadline for the request is the end of August 2021, the project is also conducting consultations to the extent possible in preparation for submitting the official request.
	High	

Among these, the following had a particular impact on the implementation and outcome of the project.

6. Delay in equipment procurement
11. Delay in approving Project Document and Signing updated R/D
12. Delays in delivery of malware analysis and evaluation lab equipment

In the second JCC, we increased the number of malware analysis equipment types and added CC evaluation equipment, which we had planned from the beginning, but the procurement of these equipment types was delayed, making it necessary to extend the project for a second time. Although COVID-19 had a significant impact on the project, it is possible that the project could have been completed within the project period if the equipment procurement had started earlier. The procurement of equipment had to wait for the approval of the project document within the Vietnamese government, which was given one year after the second JCC when the decision was made to add equipment and extend the project, so it was difficult to start the procurement early.

3. Evaluation on the results of the Project Risk Management

(1) Risk management results

Risks management results are described in “2. Key Factors Affecting Implementation and Outcome”.

(2) Results of the use of lessons learnt

The lesson learned from a similar project in the past and its application to the project was as follows.

- Lesson learned from similar projects

Under the Project on Capacity building for Information Security in Indonesia (Technical Cooperation implemented from 2014 to 2017), to improve operational capacity for information security measures in the Ministry of Communication and Information Technology in Indonesia, the Information Security Management System (ISMS) was promoted, technical training was conducted, ISMS was introduced to local government through the pilot project, a method to establish CSIRT was created, and awareness-raising was improved.

In the ASEAN countries, while the number of officers in charge of cyber security is limited, many training courses and international conferences on cyber security are held in their own country and others. The officers are busy attending to them and frequently absent from their offices. Even being in their offices, they are busy with their daily routine, and they may not be able to perform planned activities in a project.

- Application to the Project

During formulation and implementation of the plan of operations, the status of the organization and daily operation of AIS should be observed and considered. Such information should be shared with the supporting organizations in Japan, particularly the National center of Incident readiness and Strategy for Cybersecurity (NISC).

The result of the application of the lesson learned is as follows.

AIS did not share the status of the training programs other than the JICA project in advance. It was also difficult for the project to check the training status with NISC and other organizations every time. However, we were able to know the status of other training at the stage of CDP review and local training coordination, so there were no cases where trainees did not participate due to conflicts with other training.

Requesting trainees to coordinate their work through AIS executives did not prevent unexpected work from occurring.

4. Lessons Learnt

The lessons learned from this project are as follows.

(1) Methods for improving knowledge and skills over the medium and long term (for training tied to certification exams)

To consolidate the knowledge of the trainees in this project, short-term intensive training of about 5 days was followed by 3-5 months of online self-learning or coaching by instructors. In addition, trainees who scored high in online learning were offered the opportunity to take a one-time certification exam. While some certifications are considered essential for engineers' careers, it is sometimes difficult for them to take the examinations due to the high cost. In this project, we successfully motivated the participants to take the certification examinations to establish their knowledge over the medium to long term. Passing the certification exam was not the project's goal but was only offered to trainees who met the requirements to motivate them to take the exam.

(2) Preparing an environment to focus on training

In this project, 87 training sessions were conducted, with more than 600 trainees participating. Most of the trainees concentrated on the training, but some canceled at the last minute or had a low participation rate. The reasons for these were: they had work to do before and after the training day so they could not concentrate on the training, their supervisors (or vice ministers in some cases) asked them to do urgent work, they had to deal with security incidents, or the training was not what they were looking for.

When implementing intensive training in future technical cooperation projects, it is desirable to address each factor.

- Dealing with normal work

  Since most of the training took place in Hanoi, where the trainees' workplaces are located, the trainees could return to their work easily. Trainees traveling from regional cities seemed to concentrate on their work, partly because they were away from their workplaces. Requests made to the trainees themselves and the managers of their organizations to make adjustments to concentrate on the training were sometimes not adequately implemented. Depending on the pace at which the training is conducted and the budget, it is advisable to conduct the training in an overnight stay away from the workplace to concentrate on the training.

- Co-design of training content

  The custom training program should be designed with the trainees, taking time to design the content together. In this way, there will be fewer opinions about the content after the training starts.

(3) Use of local and Japanese resources

This project used local resources for most of the local training, surveys, portal development, and video production. Especially for training and consulting, even if it was limited to cyber security, a certain level of human resources existed in the cooperating countries, and they were able to provide necessary cooperation for various needs of this project. In cases where local resources could not address issues or where Japanese experience was needed, Japanese experts provided guidance, enabling the activities to be carried out while maintaining a balance between cost, procurement, and human resources. In future technical cooperation projects on cyber security (broadly, in the ICT field), it is desirable to consider the possibility of using local resources fully. In the case of local resources, the cost can be kept low, and the time to contract can be shortened. In addition, if they can speak the local official language, communication will be smoother, and they can concentrate on the content.

(4) Equipment procurement process in Viet Nam

A total of 201 pieces of equipment (146 hardware and 55 software) were procured for this project. After coordinating the equipment specifications with counterpart, the specifications were described in the project document, an internal document of the Vietnamese government. And after approval, the equipment procurement was started. It was necessary to procure the equipment according to the specifications described in the project document, however the following problems occurred during the procurement process.

- It took several months for approval, and the time lag between specification determination and procurement made the original specifications obsolete.
- It was only at the procurement stage that the information on products sold in Vietnam became clear.
- The specifications that had been omitted at the procurement stage were clarified. (country of

production, etc.)

- There were cases where the vendor did not propose the model we were looking for, although the specifications for CPU, memory, etc., were met.

As a result, it took a long time to make adjustments, and we could not procure everything within the initial project period. In addition, we were unable to provide sufficient technical support for equipment installation and operation. It inevitably takes time to approve project documents. It is also common in IT system development that the requirements change, and the specifications become outdated as time passes.

One of the reasons for the problem seems to be that the specifications in the project documents and the actual procurement documents were written as if they were the same. Therefore, it is recommended that the following measures be taken when providing equipment for future technical cooperation projects in Viet Nam. This will help to maintain consistency between the project document and procurement documents and reduce rework.

- The project document should contain only the minimum specifications for the type of equipment (workstation, storage, etc.), CPU, memory, etc.
- At the procurement stage, specify the specific model, country of origin, etc., while meeting the specifications described in the project document.

IV. For the Achievement of Overall Goals after Project Completion

1. Prospects to achieve Overall Goal

For the overall goal, refer to “III. Results of Joint Review 1. Results of Review based on DAC Evaluation Criteria: 1-4. Impact”. This section discusses the appropriateness of the indicators for the overall goal.

The indicator for the overall goal was set as a periodic report issued by the AIS, but this report was not issued between the start and the end of the project. Therefore, it is not possible to determine the achievement status of the upper-level targets. On the other hand, in 2021, the Vietnamese government aimed to improve the Global Cybersecurity Index (GCI) regarding cyber security. If the assessment items of the CGI reflect the achievements of AIS missions that are expected to contribute to the high-level goals, the CGI could be added as one of the indicators.

2. Plan of Operation and Implementation Structure of the Vietnamese side to achieve the Overall Goal

The implementation structure of the AIS for each mission involved in the project to achieve the overall goal is as follows. The policies and plans related to these missions are described in Vietnam's policies described in “ III. Results of Joint Review 1. Results of Review based on DAC Evaluation Criteria: 1-1. Relevance”.

Mission	Organization in charge
Common Criteria Evaluation system establishment	VNCERT/CC (Inspection Division)
COP policy implementation	VNCERT/CC (Inspection Division)
ISAC establishment	AIS (Threat Intelligence Division)
CSIRT operation	NCSC, VNCERT/CC
TSUBAME operation	VNCERT/CC

3. Recommendations for the Vietnamese side

The following recommendations have been made to the AIS through the project activities for sustainable capacity building on cyber security. Details are not provided here, but it is recommended that these be prioritized and addressed to achieve the overall goal.

3-1 Continuous operation of the CDP method

It is challenging to continue the methods implemented by the project as they are with few resources. However, it is advisable to consider partial implementation using one of the deliverables, such as the CDP manual, to provide systematic training with career awareness.

3-2 ISAC Establishment

A report on the survey results of ISAC establishment operations in Viet Nam's neighboring countries has been prepared by Vietnet-ICT. This report includes specific recommendations from consultants based on the survey results. It can be used as a reference for future ISAC establishment in Vietnam.
Japanese financial ISAC and ICT-ISAC held seminars to share Japanese knowledge and experiences. It is advisable to refer to the seminar materials and recommendations from Japanese experts to establish ISAC.

3-3 Promotion of COP Policy

The project team conducted seminars on Japan's awareness-raising activities, educational materials, and marketing techniques. In addition, JICA experts provided advice on the master plan for public awareness and AIS's policies. In particular, the COP policy will continue to be an essential policy of the AIS and will significantly impact the people, so it is desirable to make concrete use of the project's findings.

3-4 Operation and management of equipment

It is desirable to manage the user and status of the equipment as part of asset management. In addition, since analysis tools, etc., have an expiration date, it is desirable to secure renewal costs for continued use.

3-5 IT Security Evaluation System in Viet Nam

We have provided much information on the evaluation system through training and consulting. It is desirable to start with the provisional operation of a simple evaluation system using the equipment provided. In parallel, it is also desirable to promote membership in the CCRA.

3-6 TSUBAME Operation

In the CSIRT training conducted by JPCERT/CC in June 2021, operational advice by TSUBAME and information on vulnerabilities in Viet Nam were shared. By systematically implementing this advice, it is expected that the ability to collect threat information and respond to vulnerabilities will be improved.

4. Monitoring Plan from the end of the Project to Ex-post Evaluation

JICA will remotely monitor the operation status of the equipment (malware analysis and Common Criteria evaluation equipment) that was provided late and the quality of the dissemination and awareness-raising materials due to their enormous impact on the public every quarter (3 months) by e-mail.

<Items to be checked>

1. Operational status of malware analysis equipment
2. Operational status of Common Criteria evaluation equipment
3. Status of the utilization of awareness-raising materials (animation videos, design kit, portal site)
4. Status of the utilization of knowledge and training materials obtained from the training, etc.

ANNEX

1. Plan of Operation (PO)
2. Project Design Matrix (PDM)
3. List of Dispatched Experts
4. Relationship between Activity and Output
5. Example of CDP form (filled sample)
6. List of Trainings
7. Mapping between Project Output and Training
8. List of Products Produced by the Project
9. Training Result
10. Feedback from Trainees
11. Equipment List
12. Activities, Inputs, and Outputs for Each Outcome
13. R/D, M/M (copy)
14. Monitoring Sheet (copy)
15. Joint Coordination Committee (JCC)
16. A collection of comments from the CDP review

ANNEX 1: Plan of Operation (PO)

PO is attached

ANNEX 2: Project Design Matrix (PDM)

PDM version 1 (signed on 8th March 2019) is attached

PDM version 2 (signed on 24th August 2021) is attached

PDM version 3 (signed on XX March 2022) is attached

ANNEX 3: List of Dispatched Experts

Planned		Actual Progress
	Long-Term	
	Cybersecurity / Project Coordinator	Role: Coordinating the project. Dispatched on 26th June 2019 until 14th March 2022.
	Short-Term *added at the 2nd JCC	
	Chief Advisor	Role: Supervising the JICA expert team. Not dispatched, advising from Tokyo.
	Cybersecurity / Career Development Plan	Role: Creating and reviewing career development plans and supporting all activities of the project. 1st dispatch: 28th July – 25th September 2019 (60 days) 2nd dispatch: 6th November – 10th December 2019 (35 days) 3rd dispatch: 25th November 2021 to 22nd January 2022. 3rd dispatch was postponed due to the CoVID-19 spread. During this term, the expert has been conducting all activity online.
*	Information Sharing Analysis Center (ISAC)	Role: Support for establishment of ISAC as a part of training activity. The expert has been conducting all activity online.
*	Awareness Raising for Child Online Protection	Role: Survey for awareness raising in Japan, and training. The experts have been conducting all activity online.

The following experts were not planned on the PDM, however they cooperated with the project through seminar or training online.

National center of Incident readiness and Strategy for Cybersecurity (NISC), Ministry of Internal Affairs and Communications (MIC), Ministry of Economy, Trade and Industry (METI), Meiji University, JPCERT/CC, Information-technology Promotion Agency, Financial-ISAC, ICT-ISAC, ECSEC Laboratory Inc., Armoris Co., Ltd., Ushijima & Partners, Attorneys-at-Law

ANNEX 4: Relationship between Activity and Output

No	Activity	Output 1	Output 2	Output 3
1	Clarify the required roles defined in SecBoK framework	1.1	-	-
2	Develop a Career Development Plan (CDP) for each staff based on SecBoK Framework	1-2	-	-
3	Develop a training course plan for high prioritized roles defined in SecBoK Framework	1-3 CISO, Commander, etc.	2-1 Incident manager, Incident handler, Triage, etc.	3-1 Researcher, Solution analyst, Vulnerability diagnostic consultant, Information security auditor, etc.
4	Conduct training	1.4	2-2	3-2
5	Review CDP (e.g., every six months)	1.5	2-3	3-3
6	Plan and conduct training for policy maker	1-6	-	-
7	Develop/localize awareness raising materials	1-7	-	-
8	Expand reactive and proactive infrastructure in AIS	-	2-4 reactive infrastructure (e.g., DDoS attack mitigation)	3-4 proactive infrastructure (e.g., network monitoring)

ANNEX 5: Example of CDP form (filled sample)

CAREER DEVELOPMENT PLAN [DDDD]

LAST UPDATE: 10 Feb 2022

Name	Mr. Sample	CDP-ID	CDP-X-XXX

1 Division & Title

Division: Monitoring & Incident Response

Title: N.A.

2 Job Description, Responsibility

(1) Monitoring Server, PCs, Networks. Execute the monitoring tasks in real-time in order to provide notification, alert or warning in time.

(2) Support evaluating infrastructure of clients (NCSC's business).

3 Assigned Security Role(s)

□ CISO □ POC (Point of Contact) □ Notification □ Commander ■ Triage
□ Incident manager ■ Incident handler □ Curator □ Researcher □ Self assessment
□ Solution analyst □ Vulnerability diagnostic consultant □ Education / Awareness raising
□ Forensic engineer □ Investigator □ Legal advisor □ IT planning division
■ IT system division □ Information security auditor □ Licensing □ Policy making
■ SOC (Security Operation Center)
□ Other ( ) ■=marked

4 Required Knowledge and Skills for the Roles (General description)

(1) Knowledge of networking and Internet communications fundamentals (i.e. devices, device configuration , hardware, software, applications, ports/protocols, addressing, network architecture and infrastructure, routing, operating systems, etc.).

(2) Skill & understanding of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump). Insight of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.

(3) Understanding of crisis management protocols, processes, and techniques. Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems.

5 Knowledge and Skills to be acquired or improved

To the date of the 2nd review, he has get more progression in his career path in AIS also. Now he is primary official responding to the infrastructure services. He will keep on track with latest Linux foundation to manage the servers with LPIC-1 training, heading towards LPIC-2 if possible. Starting from Dec 2020, English training for the A2 level (CEFR) brings him two sessions per week with native speaker, also with customized content in cybersecurity. In preparation for a dynamic future of his career, Certified SOC Analyst (CSA) is assigned to him within next 6 months. Per his good performance, CEH is also added after the 3rd review.

6 Training plan, progress and result

No.	Course Title	Code	Vendor	Course provider	Planned Month	Attending Date		# hours	Cert.	Progress	Remark
						From	To				
e.g.	CompTIA Security Plus	CompTIA S+	CompTIA	XXX Corp.	Dec 2019	1 Dec 2019	7 Dec 2019	40	Passed	100%	Memo
1	Certified Network Associate	CCNA	Cisco	iPMAC	Jan 2020	13 Jan 2020	17 Jan 2020	40	Failed	70%	
2	Certified Security Specialist	ECSS	EC-Council	iPMAC	Mar 2020	02 Mar 2020	27 Mar 2020	40	Passed	70%	
3	VMware: vSphere Install, Config, Manage	VCP-DCV 1	VMware	Qnet	Nov 2020	30 Nov 2020	04 Dec 2020	40	Passed	100%	
4	VMware: vSphere Optimize & Scale	VCP-DCV 2	VMware	Qnet	Dec 2020	21 Dec 2020	25 Dec 2020	40	Passed	100%	
5	Linux Administrator	LPIC-1	LPI	SaigonCTT	Apr 2021	22 Apr 2021	29 Apr 2021	40	In Progress	80%	completed 11 times but avg. score is about 92.00 in June 2021.
6	*CSIRT organization, process and activity	CSIRT	Custom	JPCERT/CC	Jun 2021	15 Jun 2021	18 Jun 2021	24	N/A	75%	
7	Certified SOC Analyst	CSA	EC-Council	iPMAC	Jun 2021	21 Jun 2021	06 Jul 2021	40	Passed	100%	
8	Certified Ethical Hacker	CEH	EC-Council	iPMAC	Sep 2021	20 Sep 2021	24 Sep 2021	40	Failed	100%	
9	*Business English Course for Cybersecurity Beginner	ESP-BEG	Custom	Language Link	Dec 2020	01 Dec 2020	01 Jun 2021	48	Passed	75%	
10											
11											
12											
13											
14											
15											

1/2 CDP Form Rev.08

PROGRESS REVIEW

Name	Mr. Sample	CDP-ID	CDP-X-XXX

1	**Review 1**	[Date	11 Jun 2020	
	His Infrastructure management task is now covered for both server and network. He found out the ECSS is more simpler than CCNA S. For the CCNA S, he found new knowledge which could master the skill & harden the current AIS system and evaluating clients' system.			
2	**Review 2**	[Date	14 Dec 2020	
	No change in his position, but his task list are huge now because a senisor guy who was primary in charge for the infrastructure moved out of AIS. Now he and one new official are assigned to work as system admin. He enjoys the English class with native speaker, also appreciates the training for virtualization technology as a helpful chance to consolidate his knowledge for the daily tasks. The continuous connection with trainer is also advantage to give him supportive resources after the training.			
3	**Review 3**	[Date	11 May 2021	
	LPIC-1 helps him to enhance his knowledge about the Linux operating system. VMware is also one of his familiar area, but the training is also helpful to him e.g. Virtual SAN, network. English (LL) course is quite simple for him, the approach for training is fine. For the next six month, CEH is added to support for further incident response activity.			
4	**Review 4**	[Date	29 Nov 2021	
	Within two years, he has joined several trainings, and having understanding in several courses. The course helped him to understand the procedures in incident response. The whole course seems to help him see the policy than the technical training. He will try to take the LPIC-1 exam within December 2021. It seems the new CEH exam was tough for him, but he has gained the core value from the intensive training.			
5	**Review 5**	[Date		]
6	**Review 6**	[Date		]
7	**Review 7**	[Date		]

ANNEX 6: List of Trainings

No	Category	Course Name	Vendor	Training Institutes	Date
1	General Security knowledge	CompTIA Security +	CompTIA	NetPro NetPro SaigonCTT NetPro NetPro	September 2019 June 2020 June 2020 October 2020 September 2021
		Certified Security Specialist (ECSS)	EC-Council	iPMAC iPMAC iPMAC iPMAC iPMAC iPMAC	Mar 2020 May 2020 October 2020 April 2021 August 2021 October 2021
2	Network, Network Security	Cisco Certified Network Associate (CCNA)	Cisco	NetPro	May 2021
		Cisco Certified Network Professional Security (CCNP Security)	Cisco	NetPro NetPro	January 2020 January 2020
3	Security Manager, Auditor	Certified Information Systems Security Professional (CISSP)	(ISC)2	iPMAC	June 2021
		Certified Information Security Manager (CISM)	ISACA	Qnet Qnet	July 2020 August 2021
		Certified Information Systems Auditor (CISA)	ISACA	iPAMC	March 2020
4	Hacking, Pentesting	Certified Ethical Hacker (CEH)	EC-Council	Cecomtech Cecomtech iPMAC iPMAC Cecomtech iPMAC iPMAC iPMAC iPMAC	December 2019 May 2020 November 2020 January 2021 April 2021 September 2021 September 2021 January 2022 January 2022
		Licensed Penetration Tester (LPT)	EC-Council	Cecomtech	August 2021
		PEN200: Penetration Testing with Kali Linux (OCSP)	Offensive Security	Cecomtech Cecomtech Cecomtech iPMAC	November 2020 May 2021 August 2021 January 2022
		Offensive Security (OSWE) | Advanced Web Attacks and Exploitation (WEB-300)	Offensive Security	Cecomtech Cecomtech	December 2021 January 2022

No	Category	Course Name	Vendor	Training Institutes	Date
5	Coding, Development	Cyber Secure Coder (CSC)	Logical Operations	Qnet	July 2021
6	Project Management	Certified Associate in Project Management (CAPM)	PMI	iPMAC	September 2020
		Project Management Professional (PMP)	PMI	iPMAC iPMAC iPMAC iPMAC	August 2020 September 2020 October 2021 January 2022
7	Infrastructure	Linux Administrator (LPIC-1)	LPI	SaigonCTT SaigonCTT	June 2020 April 2021
		VMware: vSphere Install, Config, Manage	VMware	Qnet	November 2020
		VMware: vSphere Optimize & Scale	VMware	Qnet	December 2020
8	Threat Intelligence	Certified Threat Intelligence Analyst (CTIA)	EC-Council	iPMAC iPMAC	May 2021 January 2022
9	SOC, CSIRT	Certified SOC Analyst (CSA)	EC-Council	iPMAC iPMAC	June 2021 August 2021
		Defense Practice against Cyber Attacks	Training in Japan (online)	JICA	September 2020 February 2021 November 2021
		CSIRT organization, process and activity	Custom	JPCERT/CC	July 2021
		Cyber Exercise	Custom	Cecomtech	November 2021
		Building and Operation of Cyber Exercise	Custom	JICA	January 2022
10	Forensics, Malware Analysis	Malware Analysis	Custom	JPCERT/CC	December 2021
		Malware Analysis Tools	Custom	iPMAC	February 2021
		Computer Hacking Forensic Investigator (CHFI)	EC-Council	Cecomtech Cecomtech NetPro	July 2020 June 2021 September 2021
11	Policy, Regulation, Governance	Security Policy Making	Custom	JICA	June 2021
		Capacity Building in Policy Formation for Enhancement of Measures to Ensure Cybersecurity in ASEAN Region	Training in Japan	JICA	February 2020
		Capacity Building in International Law and Policy Formation for Enhancement of Measures to Ensure Cybersecurity	Training in Japan (online)	JICA	October 2021
12	Awareness Raising	Awareness raising seminar	Custom	JICA	August 2021
13	International Standard	International Standards: ISO/IEC 27000 family	Custom	SaigonCTT	March 2021
		International Standards: US NIST SP800	Custom	NetPro	September 2021
		International Standards: GDPR	Custom	iPMAC	November 2021

No	Category	Course Name	Vendor	Training Institutes	Date
14	Security Evaluation	International Standard: Common Criteria	Custom	Individual	August 2020
		International Standard: ISO/IEC 17025	Custom	SmartPro	February 2021
		Security Evaluation Online Seminar	Custom	JICA	February 2021 March 2021
		Common Criteria (Protection Profile-Security Target-Target of Evaluation)	Custom	SmartPro	July 2021 August 2021
		Evaluation Lab Operation	Custom	SmartPro	January 2022
15	Critical Information Infrastructure	ISAC Online Seminar	Custom	JICA	February 2021
		JP-US Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region	Training in Japan (online)	METI	March 2021 October 2021
		Critical Information Infrastructure Protection	Custom	NetPro	November 2021
		Industrial Control Systems Cybersecurity Training for Indo-Pacific Region	Training in Japan (online)	JICA Tokyo	February 2021
		Strengthening of Cooperation Among Organizations Against Cyberattacks	Training in Japan (online)	JICA Tokyo	February 2021
16	English	Business English Course for Cybersecurity 1 (HN)	Custom	British Council	October 2020 – December 2021
		Business English Course for Cybersecurity 2 (HN)	Custom	ILA	December 2020 – August 2021
		Business English Course for Cybersecurity 3 (HN)	Custom	British Council	October – December 2021
		Business English Course for Cybersecurity 4 (HCMC)	Custom	British Council	November – December 2021
17	Training in Third Country	Third country training in Indonesia	Training in third country	JICA	December 2019

ANNEX 7: Mapping between Project Output and Training

◎: Most strongly related
○: Related

No	Category	Course Name	Output 1 Management	Output 2 Reactive	Output 3 Proactive
1	General Security knowledge	CompTIA Security +	◎	◎	◎
		ECSS	◎	◎	◎
2	Network, Network Security	CCNA	◎	◎	◎
		CCNP Security	◎	◎	◎
3	Security Manager, Auditor	CISSP	◎	○	○
		CISM	◎	○	○
		CISA	◎	○	○
4	Hacking, Pentesting	CEH			◎
		LPT			◎
		OCSP			◎
		OSWE			◎
5	Coding, Development	CSC		○	○
6	Project Management	CAPM	◎	○	○
		PMP	◎	○	○
7	Infrastructure	LPIC-1	○	○	◎
		VMware: vSphere Install, Config, Manage	○	○	◎
		VMware: vSphere Optimize & Scale	○	○	◎
8	Threat Intelligence	CTIA			◎
9	SOC, CSIRT	CSA			◎
		Defense Practice against Cyber Attacks		◎	
		CSIRT	○	◎	◎
		Cyber Exercise	○	◎	◎
		Building and Operation of Cyber Exercise	○	◎	◎
10	Forensics, Malware Analysis	Malware Analysis		◎	
		Advanced Malware Analysis		◎	
		CHFI		◎	
11	Policy, Regulation, Governance	Security Policy Making	◎		
		Capacity Building in Policy Formation in ASEAN Region	◎		
		Capacity Building in International Law	◎		

No	Category	Course Name	**Output 1** Management	**Output 2** Reactive	**Output 3** Proactive
12	Awareness Raising	Awareness raising	◎		○
13	International Standard	ISO/IEC 27000 family	◎		○
		US NIST SP800	◎	◎	◎
		GDPR	◎		
14	Security Evaluation	Common Criteria	○		◎
		ISO/IEC 17025			◎
		Security Evaluation Online Seminar			◎
		Common Criteria (PP-ST-TOE)			◎
		Evaluation Lab Operation			◎
15	Critical Information Infrastructure	ISAC Online Seminar	○		◎
		JP-US Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region		◎	◎
		CIIP	◎	◎	◎
		Industrial Control Systems		◎	◎
		Strengthening of Cooperation		◎	◎
16	English	Business English for Cybersecurity	◎	◎	◎
17	Training in Third Country	Third country training in Indonesia	○	◎	○

ANNEX 8: List of Products Produced by the Project

No.	Products	Related Activity
1	CDP format	1-1. 1-2. 1-3. 1-5. 2-1. 2-3. 3-1. 3-3.
2	CDP manual	
3	Created CDPs	
4	CDP portal site	
5	Training materials	1-4. 1-6. 2-2. 3-2.
6	ISAC survey report	3-2.
7	Animation video 1	1-7.
8	Animation video 2	
9	Animation video 3	
10	Branding kit (Logo, slogan, etc.)	
11	COP portal site	
12	Lab Security Manual	3-4.
13	Security Evaluation Procedure (lightweight)	
14	Security Evaluation Procedure (EAL2+ Common Criteria)	
15	Evaluation Template	

ANNEX 9: Training Result

- **Comparison of pre-test, post-test and certification exam**

No.	Course	Month Year	Training			Online Practice		Certification Exam		
			Planned Num. of trainee	Actual Num. of trainee	Increased point (pre vs post-test)	Actual Num. of trainee	Increased point (pre vs online-test)	Examinees	Passed	Increased point (pre vs exam test)
1	CompTIA S+ Gr1	09/2019	4	4	**12.59**	-	-	4	1	34.00
2	CEH Gr1	12/2019	6	4	**20.08**	-	-	4	4	32.98
3	CCNA Security Gr1	01/2020	6	3	**16.42**	2	52.92	0	0	-
4	CCNA Security Gr2	01/2020	6	6	**3.33**	6	65.42	3	0	36.02
5	ECSS Gr1	04/2020	7	8	**31.43**	8	55.37	8	7	46.12
6	ECSS Gr2	05/2020	10	9	**32.94**	5	43.69	6	5	48.11
7	CEH Gr2	05/2020	8	7	**6.47**	5	25.85	7	7	27.90
8	CompTIA S+ Gr2	05/2020	5	4	**21.35**	2	20.78	1	1	(pending)
9	CompTIA S+ Gr3	06/2020	5	6	**3.92**	3	26.42	1	0	32.86
10	LPIC-1 Gr1	07/2020	6	5	**29.08**	3	23.98	0	0	-
11	CHFI Gr1	07/2020	5	4	**4.17**	4	24.17	4	4	0.84
12	CISM Gr1	08/2020	6	6	**20.00**	5	59.86	5	1	14.01
13	PMP Gr1	08/2020	5	5	**19.55**	0	0	0	0	-
14	CAPM	08/2020	8	8	**17.70**	2	-2.38	1	1	(pending)
15	PMP Gr2	09/2020	8	7	**23.49**	0	-	0	0	-
16	ECSS Gr3	10/2020	9	4	**30.07**	1	70.07	1	1	(pending)
17	CompTIA S+ Gr4	10/2020	10	10	**3.16**	5	33.49	6	5	21.03
18	OSCP Gr1	10/2020	4	4	**-6.10**	4	-	4	3	-
19	CEH Gr3	11/2020	5	5	**5.27**	4	22.78	4	4	(pending)
20	VCP-1	12/2020	5	5	**6.33**	4	19.47	5	5	(pending)
21	VCP-2	12/2020	5	5	**16.26**					
22	CEH Gr4	01/2021	5	6	**29.00**	5	64.83	5	3	(pending)
23	CISA	03/2021	6	6	**54.50**	4	(pending)	2	2	(pending)
24	ECSS Gr4	04/2021	15	15	**66.03**	15	(pending)	15	15	48.36
25	CEH Gr5	04/2021	5	5	**19.40**	5	30.90	5	2	9.20
26	LPIC-1 Gr2	05/2021	8	8	**41.67**	6	(pending)	6	(pending)	(pending)
27	OSCP Gr2	05/2021	4	4	**23.60**	4	-	4	3	-

No.	**Course**	**Month Year**	**Training**			**Online Practice**		**Certification Exam**		
			Planned Num. of trainee	**Actual Num. of trainee**	**Increased point (pre vs post-test)**	**Actual Num. of trainee**	**Increased point (pre vs online-test)**	**Examinees**	**Passed**	**Increased point (pre vs exam test)**
28	CTIA Gr1	05/2021	10	10	**5.65**	3	(pending)	8	8	-
29	CCNA	05/2021	5	5	**12.33**	5	(pending)	5	5	(pending)
30	CHFI Gr2	05/2021	10	10	**10.13**	10	(pending)	10	10	(pending)
31	CSA Gr1	05/2021	7	7	**19.11**	7	(pending)	7	7	(pending)
32	CISSP	06/2021	6	6	**-7.86**	2	(pending)	2	1	(pending)
33	CompTIA S+ Gr5	07/2021	7	7	**10.63**	6	(pending)	6	4	13.72
34	CSC	07/2021	7	7	**-5.04**	5	(pending)	5	0	(pending)
35	ECSS Gr5	08/2021	11	11	**25.45**	9	(pending)	9	9	34.79
36	CSA Gr2	08/2021	7	7	**3.35**	6	(pending)	6	6	32.41
37	OSCP Gr3	08/2021	4	4	**15.74**	4	-	2	1	-
38	LPT	08/2021	5	5	**-5.70**	5	(pending)	(pending)	(pending)	(pending)
39	PMP Gr3	08/2021	7	7	**30.00**	1	(pending)	1	0	(pending)
40	CISM Gr2	08/2021	5	5	**-29.80**	3	(pending)	2	2	(pending)
41	CHFI Gr3	09/2021	5	5	**14.86**	1	(pending)	1	1	(pending)
42	CEH Gr6	09/2021	8	8	**17.19**	8	(pending)	8	8	24.59
43	CEH Gr7	09/2021	6	6	**0.83**	6	(pending)	6	6	9.30
44	PMP Gr4	10/2021	9	9	**8.89**	1	(pending)	1	0	(pending)
45	ECSS Gr6	10/2021	7	7	**25.35**	7	(pending)	7	6	35.43
46	OSWE Gr1	12/2021	4	4	**-23.43**	4	(pending)	(pending)	(pending)	(pending)
47	CEH Gr8	01/2022	9	9	**23.89**		(pending)	(pending)	(pending)	(pending)
48	PMP Gr5	01/2022	8	8	**17.50**	(pending)	(pending)	(pending)	(pending)	(pending)
49	OSWE Gr2	01/2022	4	4	**8.57**	4	-	-	(pending)	-
50	CEH Gr9	01/2022	7	7	**14.64**	(pending)	(pending)	(pending)	(pending)	(pending)
51	CTIA Gr2	01/2022	8	8	**-0.31**	(pending)	(pending)	(pending)	(pending)	(pending)
52	OSCP Gr4	01/2022	4	4	**-3.33**	4	(pending)	(pending)	(pending)	-
	Total	**-**	**346**	**333**	**-**	208	-	185	147	-

- **Custom course**

No.	Course	Month Year	Training		
			Planned Num. of trainee	**Actual Num. of trainee**	**Increased point (pre vs post-test)**
1	Common Criteria	06/2020	12	11	18.68
2	Business English for Cybersecurity Group 1	12/2020	13	14	-
3	Business English for Cybersecurity Group 2	12/2020	19	18	-
4	ISAC Online Seminar	02/2021	10	10	-
5	ISO 17025	02/2021	9	10	3.00
6	Security Evaluation Online Seminar 1	02/2021	12	12	-
7	ISO 27000 family	03/2021	12	10	24.70
8	Security Evaluation Online Seminar 2	03/2021	9	8	-
9	CSIRT Training	05/2021	11	11	-
10	Common Criteria (PP, ST, TOE) 1	07/2021	9	8	-1.60
11	Policy making Seminar	07/2021	31	27	-
12	Common Criteria (PP, ST, TOE) 2	08/2021	9	5	-43.06
13	Awareness-raising	08/2021	18	14	-
14	NIST SP800	09/2021	20	17	18.30
15	Business English for Cybersecurity Group 3 (Hanoi)	10/2021	17	17	-
16	Business English for Cybersecurity Group 4 (HCMC)	11/2021	13	12	-
17	ISAC Meeting	11/2021	3	3	-
18	GDPR	11/2021	13	12	-4.40
19	CIIP	11/2021	13	8	6.10
20	Cyber Exercise	12/2021	14	14	2.00
21	Python Programming	12/2021	6	6	10.60
22	JPCERT/CC Malware Analysis	12/2021	15	20	-
23	Building and Operation of Cyber Exercise	01/2022	17	17	-
24	Evaluation Lab Operation	01/2022	3	3	-
25	Malware analysis tool	02/2022	15	15	-
	Total		**323**	**302**	

- **Other Training Course (Training in Japan, Training in Third Country)**

			Training		
No.	**Course**	**Month Year**	**Planned Num. of trainee**	**Actual Num. of trainee**	**Increased point (pre vs post-test)**
1	Training in Indonesia	09/2019	4	3	-
2	Capacity Building in Policy Formation for Enhancement of Measures to Ensure Cybersecurity in ASEAN Region	02/2020	2	2	-
3	Defense Practice against Cyber Attacks	09/2020	1	1	-
4	Defense Practice against Cyber Attacks	02/2021	1	1	-
5	JP-US ICS Cybersecurity Week	03/2021	2	2	-
6	JP-US ICS Cybersecurity Week FY2021	10/2021	2	2	-
7	International Law 2021	10/2021	2	2	-
8	Defense Practice (A) 2021	11/2021	1	1	-
9	Industrial Control Systems Cybersecurity Training for Indo-Pacific Region	02/2022	2	2	-
10	Cooperation Among Organizations Against Cyberattacks 2022	02/2022	1	1	-
	Total		**18**	**17**	

ANNEX 10: Feedback from Trainees

- **Feedback from Trainees (cumulative data)**

		Total				
Options**: Strongly Agree (A), Agree (B), Neutral (C), Disagree (D), Strongly Disagree (E)**		E	D	C	B	A
1	The trainer was knowledgeable about the training topics.	1	0	19	101	99
2	The trainer was professional and well prepared.	0	9	17	85	108
3	The trainer helped when I had difficulty understanding the content or performing activities	0	2	25	102	91
4	The trainer promptly answered questions and provided constructive feedback.	0	0	25	93	102
5	The objectives of the training were clearly defined.	0	1	23	93	104
6	Participation and interaction were encouraged.	0	2	28	102	89
7	Overall, the trainer exceeded my expectations.	0	12	27	110	72
8	The training room and facilities were adequate and comfortable.	0	0	14	135	72
9	The topics covered were relevant to me.	0	0	15	137	69
10	The content was organized and easy to follow.	1	0	36	112	72
11	The training activities helped me understand the content provided.	0	12	25	98	86
12	The materials distributed were helpful.	0	2	26	112	81
13	The training objectives were met.	0	13	21	120	67
14	The time allotted for the training was sufficient.	0	8	37	112	64
15	This training experience will be useful in my work.	0	11	15	110	85
16	The training experience encouraged me to seek out future training courses.	0	2	19	132	68
17	Overall, I am satisfied with the results of the training course	0	13	15	118	75
18	Further comments in example: “The training provides me practical knowledge about current working environment? It helps me prevent making mistakes at work place via organized content and activities.”					

- Further Comments from Trainees

CompTIA Security+ training (group 1)	
	Yes. (answer for the example)
	It helps me prevent making mistakes at workplace via organized content and activities
	yes, i think so (answer for the example)
CEH training (group 1)	
	The training provides me practical knowledge about current working environment.
	I think it is such a good choice I make. It helps me know the key points about CEH
	We I need more time to prepare for the upcoming exam
	the training provides me new knowledge, help me in my work. i hope have many more time to learn and practice
CCNA Security training (group 1)	
	No Comment
CCNA Security training (group 2)	
	In my current working environment, we using a lot of network equipment from cisco and the other products. After this training, we know how to protect my
ECSS training (group 1)	
	Mr. Giang (trainer) is a good teacher with great enthusiasm. The staff at IPMAC also communicates regularly and provides good student support.
ECSS training (group 2)	
	No Comment
CEH training (group 2)	
	The training provides me practical knowledge about current working environment.
	The training brings me more useful knowledges and get clearer about risks existing on cyber environment. It is good for me to work as Government officer in making regulation and policy later.
CompTIA Security* training (group 2)	
	Thank you very much to all of you.
	The training is very useful and effecive, especially materials for the course, such as exercises, video and labs with a 3-month period in Comptia website. It gives me more knowledge about theory and practices in the field of security.
CompTIA Security* training (group 3)	
	The training provides me a lot of knowledge. It helps me a lot in my current job, understands more technical information, makes it easier to analyze my technical work.
LPIC-1 training (group 1)	
	No comment
CHFI	
	Responder 01: The CHFI course provides a strong baseline knowledge of key concepts and practices in the digital forensic for me.

CISM (group 1)	
	Responder 01: I know overview of information security management and update my knowledge to keep pace with rapid changes in the management, design, oversight and assessment of information security. I will going to apply it much in my job. Responder 02: It helps me see the overview of cybersecurity, not just technical part. Responder 03: The training provides me practical knowledge in information security management. Studying more on this course will give me the way to do right in daily activities.
PMP (group 1)	
	No comment
CAPM (group 1)	
	Responder 01: The training provides me practical knowledge about current working environment. Responder 02: Yes, I do.
PMP (group 2)	
	Responder 01: Thank you JICA for organization this course. Responder 02: Not completely, However its supported me in part of the work. Responder 03: Not completely, However its supported me in part of the work.
ECSS (group 4)	
	Responder 01: The training course has provided me with practical experience. It helps me avoid mistakes at work. Responder 02: The training course has provided me with practical experience. It helps me avoid mistakes at work. Responder 03: The course is very helpful, however, I prefer training in designing policies for further Responder 04: It helps me prevent making mistakes at work place via organized content and activities.
CompTIA S+ (group 4)	
	No comment
OSCP (group 1)	
	(Pending)
CEH (group 3)	
	(Pending)
VCP-1	
	(Pending)
VCP-2	
	(Pending)
CEH (January 2021)	
	Responder 01: "I know an overview of security Certified Ethical Hacker (CEH) , provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach I how hackers think and act so you will be better positioned to set up your security infrastructure and defend against attacks." Responder 02: "good"

CISA (March 2021)	
	Besides knowledge and methodology of the course, the training should provide more templates that can be used in actual activities. For example, an full set of forms and templates to use in audit the information system of an organization.”
ECSS (April 2021)	
	Responder 01: “It is wonderful to take this course. Thank you to the Organizing Committee” Responder 02: “The training helped me increase my knowledge. I had a lot of interesting experiences with IT. Thank JICA very much!” Responder 03: “The training provides me practical knowledge about current working environment?. It helps me prevent making mistakes at work place via organized content and activities” Responder 04: “Perfect” Responder 05: the training has provide me more practical knowledge which will help me be more careful in working, as a result it might be safer for me and my assigned tasks.
CH (April 2021)	
	Responder 01: “Yes of course the training was improved my skill and very useful for my incident response career. I would like to thank JICA for giving me the opportunity to study to improve my work.” Responder 02: “This course is very helpful for my work and I love it” Responder 03: The training has provided me more practical knowledge about current working environment. It helps me prevent making mistakes at workplace via organized content and activities.
LPIC-1 (May 2021)	
	Responder 01: “The training provides me prevent making mistakes at work place via organized content and activities. Thanks!” Responder 02: “For convenience of review, for each test, the candidate should know which answer is correct”
OSCP (May 2021)	
	Responder 01: “The training help me a lot. Thanks” Responder 02: “The training provided me with more comprehensive knowledge and made it easier to work in the real world.”
CTIA (May 2021)	
	Responder 01: The training provides me practical knowledge about current working environment Responder 02: “The course covers the knowledge related to my work, support me a lot in the process of working.”
CCNA Security (June 2021)	
	Responder 01: “It is very helpful for me.” Responder 02: “The training provides me practical knowledge about current working environment.”
CHFI (June 2021)	
	Responder 01: “The training provides me practical knowledge about current working environment” Responder 02: “I think this course that is suitable for someone who want to know about forensic.” Responder 03: “the course gave me the necessary skills to identify the signs of computer network intruders, collect the necessary evidence to serve the work of continuing the investigation, thank you very much JICA” Responder 04: “It helps me prevent making mistakes at work place via organized content and activities” Responder 05: “The training is helpful and provides me more practical knowledge for working

CSA (June 2021)	
	Responder 01: "It helps me prevent making mistakes at work place via organized content and activities"
CISSP (June-July 2021)	
	Responder 01: "Thank you JICA, and IPMAC for co-operating this course." Responder 02: "this training provides me a broader view of cyber security, not only technical but also management, operation, development, It helps me prevent making mistakes at work place via organized content and activities and prove my skillset."
CompTIA Security+ Group 5	
	The training provides me practical knowledge about current working environment
ECSS Group 5	
	The training provides me practical knowledge about current working environment.
	The training provides me lots of valuable basic knowledge about information security, which is very useful for my work.
	The training helps me improve my knowledge and some skills about cybersecurity.
CSA Group 2	
	Instructors are very enthusiastic, knowledgeable and experienced. The teacher fully guides the course content, but there are many parts that the teacher has not selected and clarified the main content, and lectures regularly for the sections. The teacher teaches a lot, a little bit less interaction
	About the Lab: Instructors should choose content in mind to practice specifically. Similar posts do not need to do.
	Offer: After the course, students are provided with a lab system so that it doesn't take much time to rebuild.
OSCP Group 3	
	This training is very relevant to the reality of my work. I will try to improve my expertise and complete the certification.
LPT	
	The training provided me a lot of knowledge and experience in penetration. It will help me a lot in the process of doing related work.
	The training provides me practical knowledge about current working environment. It helps me prevent making mistakes at work place via organized content and activities
PMP Group 3	
	The course is very useful and necessary for my work in the future.
CISM Group 2	
	The time allotted for the training should have been more extended so that trainees would have more time gaining practical knowledge from trainers.
CHFI Group 3	
	The training provides me practical knowledge about current working environment.
CEH Group 6	
	The training course helped me to know new knowledge, deepen my understanding of known knowledge. At the same time, I would like to thank Mr. Pham Dinh Thang for his dedication in imparting knowledge as well as answering questions for students.

JPCERT/CC Malware Analysis	
	The training provided me with Malware knowledge and tools to analyze and identify it. It's useful.
	The training has helped me to me gain necessary knowledge for malware analysis. I could bring the absorbed knowledge into play and having fruitful outputs. Thank you JICA and experts from JPCERT, also the support team to facilitate all the favor conditions for the training. I hope to have chance attending further training in future. Thank you very much!
	In the static analysis part, I think if the training time is longer, the effect of the course will be even better.
	The training helped me better understand malware and how to analyze it. I hope to get more similar or advanced courses. Thank you.
	The training has brought the fruitful and necessary experience to detect and analyze malwares. Thanks to such effort, I could apply to the on-demand tasks with proven tracks. Please take my thanksful message to JICA, JPCERT/CC experts from Japan and organizers helping me to complete this training. I wish to attend more related training in future. Thank you very much!

ANNEX 11: Equipment List (DDoS Attack Mitigation System, Malware Analysis System, Lab for Common Criteria)

- **Package 1: DDoS Mitigation System**

No.	Equipment	Requirements	Qty.	Model
1	Servers type 1	Xeon E5-2640v3 | 128GB DDR4 | SAS 5x600GB 10k rpm | NIC 4x1Gb & 2x10Gb | PSU x2 | SAN Support	7	FUJITSU Server PRIMERGY RX2540 M5
2	Servers type 2	Xeon E3-1200 v3 | 32GB DDR3 (4x8) 1600MT/s | SAS 3x600GB 10k rpm | PSU x2 | NIC 4x1Gb	20	FUJITSU Server PRIMERGY RX1330 M4
3	Workstation	i7 6700 | 16GB DDR4 2400MT/s | Intel HD530 | HDD 1TB & SSD 512GB | NIC 1Gb	12	Workstation Fujitsu CELSIUS W5010
4	Notebook	i5 6300 | 16GB DDR4 2133MT/s | SSD 512GB SATA M.2 SED | Intel UHD620 | Intel 8265 AC & Bluetooth	5	Laptop Fujitsu LIFEBOOK U7410
5	Monitor	23.8 inch Full HD | 16:9 | 250cd/m2 | 10ms & 5ms (fast mode) | DVI-D x1 (HDCP)| VGA/DSUB x1 | Speaker | Audio in 3.5mm | USB ports x 4	30	Monitor Fujitsu FUJITSU Display P24-9 TE
6	Projector	3LCD 16mm (0,63 inch) | P-Si TFT x3 | ANSI Lumens 4200 (normal) 3444 (eco1) 2814 (eco2) | Constrast 2000:1 | Lamp life: 5000h (normal) | 8000h (eco1) | 10000h (eco2) | Manual Zoom 1.2x | Throw Distance 0.9 - 9.1m (wide); 1.0 - 10.9m (tele) | HDMI in x1 | VGA/DSUB in x2 | RCA in x1 | RS232 | Audio in	1	Maxcell MC-EX403E
7	Hard disk	SAS 300GB 6Gb 10K rpm HotPlug 2.5 EP	10	HDD SAS 12G 300GB 10K 512n HOT PL 2.5' EP
8	Hard disk	SSD 2.5 256GB SATA	5	Hard disk SSD SATA III 256GB 2.5"
9	Hard disk	SAS SSD 300GB	5	Hard disk SAS SSD 400GB
10	SAN Switch	SAN Switch: Fibre Channel ports: Switch mode (default): 24 ports or more | Scalability: Full fabric architecture with a maximum of 239 switches or more | Certified maximum: 6000 active nodes or more | 56 switches or more, 19 hops or more in Brocade Fabric OS® fabrics | 31 switches or more, 3 hops in Brocade M-EOS fabrics or more | larger fabrics certified as required | Aggregate bandwidth: 768 Gbps or more, end-to-end full duplex	2	SAN Switch Fujitsu Brocade G610
11	SAN Storage	Max raw capacity: 68.4TB system shelf, 1.7PB with disk shelves (using 1.8TB,3.2TB, and 10TB drives) | Max drives: 192 with mixed shelves, 120 SSD (25 SSD per 60-drive shelf) or bigger | Drives supported: 900GB, 1.2/1.8TB | SAS 10K | FDE/non-FDE, 1.8TB | SAS 10K FIPS, 800GB | 1.6/3.2TB or larger ; SSD non-FDE, 800GB | SSD FDE, 1.6TB | SSD FIPS | System memory: 8GB/16GB | Optional host I/O ports: 4 ports 10Gb iSCSI (copper) | 4 ports or 8 ports 10Gb iSCSI (optical) | 4 ports or 8 ports 16Gb FC | 4 ports or 8 ports 12Gb SAS.	1	SAN Storage Fujitsu Eternus DX200 S5

- **Package 2: Malware Analysis System**

No.	Equipment	Requirements	Qty.	Reference Model
1	Workstation	1U | Xeon E5-W2102 | 128GB | SSD 512GB | HDD 2x1TB | HDD 2x2TB | DVD+RW | W10 Pro | Dual monitors support | Wireless Keyboard & Mouse | 3y RMA	2	Precision 5820 Tower Custom | Convertable to Rack Mount
2	Workstation	1U | Xeon E5-W2102 | 128GB | SSD 512GB | HDD 2x1TB | DVD+RW | W10 Pro | 3y RMA	1	Precision 5820 Tower Custom | Convertable to Rack Mount
3	Server	1U | Xeon E3-1230 v6 | 128GB | SSD 512GB | HDD SATA 5x4TB (Raid 6) | Wireless Keyboard & Mouse | WS 2019 Datacenter | 3y RMA	3	DELL PowerEdge T330 Custom | Convertable to Rack Mount
4	Workstation (Client PC)	i9-10900K | 32GB DDR4 | HDD 1TB | DVD+RW | SSD 480GB | W10 Pro | 3y RMA	2	Dell OptiPlex 7080 Tower
5	Monitors	23.8 inch Full HD | 16:9 | 250cd/m2 | 10ms & 5ms (fast mode) | DVI-D x1 (HDCP) | VGA/DSUB x1 | Speaker | Audio in 3.5mm | USB ports x 4 | 3y RMA	8	Dell U2419H
6	Network device (Firewall)	2 x 1Gb RJ45 WAN | 2 x 4 SFP | 2 x 1Gb RJ45 Mgmt/HA | 14 x 1Gb RJ45 | 1 x Console RJ45 | Local Storage SSD | FW throughput (1518-byte UDP): 20 Gbps | FW throughput (512-byte UDP): 20 Gbps | FW throughput: 9 Gbps | VPN throughput (IPSec): 7200 Mbps | IPS throughput: 2200 Mbps | Threat protection throughput: 1200 Mbps | Multi-Tenant supported (VDOM) (license for 2y) | 2y RMA	2	Firewall Fortinet 200E Series
7	Network device (Switch)	24 x 10/100/1000 RJ45 PoE+ interfaces | 2 x 1Gb SFP uplinks & 2 x 10Gb SFP+ uplinks | Full duplex switching bandwidth: 254 Gbps | Forwarding rate: 68.45 Mbps | PoE Power 390W | PSU 640W | 4GB DRAM | 2048MB flash | 2y RMA	1	Cisco 3650 – 24 PDM
8	Network device (SIM)	Internet via cellular network - max speed (avg. 100Mbps Upload - Download) - unlimited bandwidth (1y subscription)	2	Mobifone
9	Network device (Gateway)	LTE CAT 20, up to 2Gbps download & 150Mbps upload | 3GPP, Rel. 14 | 5CA with 20 simultaneous Downlink layers | 4x4 MIMO | 256QAM DL / 64QAM UL CA 3C, 7C | 11ac Dual band dual concurrent | 5040mAh Battery | 1y RMA **OR** LTE CAT 6, up to 300Mbps download & 50Mbps upload | IEEE 802.11a/n/ac 5 GHz, IEEE 802.11b/g/n 2.4 GHz | 1 × 10/100/1000 Mbps LAN/WAN Port | 3 × 10/100/1000 Mbps RJ45 Ports | 1 × Micro SIM Card Slot | 2y RMA	2	Netgear Nighthawk M2 (MR2100) **OR** TP-Link Archer MR600
10	Network device (Accesspoint)	IEEE 802.11 a/b/g/n/r/k/v/ac/ac-wave2 5GHz 1733Mbps, IEEE 802.11b/g/n 2.4GHz 300Mbps | 1 × 10/100/1000 Mbps LAN PoE Port | Wireless Security: WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES), 802.11w/PMF | 2y RMA	1	JW797A Aruba AP-315 **OR** Ubiquity AP-nanoHD
11	Rack	Server Rack for Malware Analysis system's equipments >27U	1	27UD800, 27U
12	UPS	Online/Interactive UPS 5kVA | NMC controller | 2y RMA	3	APC SURTD5000XLI
13	Network device	KVM Switch for Malware Analysis system's equipments with related cables bundled (HDMI, USB, etc.) | 2y RMA	1	Tripple Lite B024-HU08

No.	Equipment	Requirements	Qty.	Reference Model
14	Software	Windows 10 Pro & Enterprise 64bit EN + Software Assurance (2y)	12	
15	Software	VMware Workstation Pro (upgradable within 2y)	5	
16	Software	Microsoft Office Professional Plus 2016 32bit (downgradable to 2013)	5	
17	Software	Visual Studio 2010 Premium with MSDN (1y)	2	
18	Software	Burp Suite Pro 1 user / 1 year	2	
19	Software	Zynamics BinDiff 5 User License	1	
20	Software	ARM64 Decompiler Fixed License [Windows]	1	
21	Software	ARM32 Decompiler Fixed License [Windows]	1	
22	Software	MIPS Decompiler Fixed License [Windows]	1	
23	Software	IDA x64 Decompiler Fixed License [Windows]	2	
24	Software	IDA x86 Decompiler Fixed License [Windows]	2	
25	Software	VB Decompiler 1 user Business License & License Update within 2y	2	
26	Software	Kaspersky Internet Security 2019	1	
27	Software	Symantec Internet Security 2019	1	
28	Software	McAfee Internet Security 2019	1	
29	Software	Veramine 1y license	1	
30	Software	Joe Sandbox Ultimate	1	
31	Software	NESSUS Pro 3y license	1	
32	Software	Cyber Triage (Team license)	1	
33	Software	IDA Pro Computer License [Windows]	2	

- **Package 3: Security Evaluation**

No.	Equipment	Requirements	Qt	Reference Model
1	Workstations	Xeon E-2124G | 32GB | HDD 2TB | NVIDIA P620 | DVD+RW | W10 Pro | 3y RMA	2	Dell Precision 3630
2	Monitors	23.8 inch Full HD | 16:9 | 250cd/m2 | 10ms & 5ms (fast mode) | DVI-D x1 (HDCP)| VGA/DSUB x1 | Speaker | Audio in 3.5mm | USB ports x 4 | 3y RMA	2	Dell Ultrasharp U2419H
3	Screen	3840 x 2160 (4x4 cabinet) | 806.4 x 453.6 x 29.9 mm (LxHxD) per cabinet | 0.8 Pixel Pitch | Flip-chip RGB LED | 2000cd/m2 | 10,000:1 | IP20 | 2y RMA **OR** 49 inch 3840 x 2160 | 16:9 | 700cd/m2 | 8ms | 4000:1 | HDMI x 2 | Display Port x 1 | DVI-D x 1 | RJ45 | Speaker | Audio in 3.5mm | USB ports x 2 | SSSP 6.0 | IP5X | VESA | 2y RMA **OR** 49 inch 5120 x 1440 | 32:9 | 350cd/m2 | 1ms & 144Hz | HDMI x 2 | Display Port x 1 |	2	Samsung LED IWJ Samsung LED QHR Samsung CRG9

No.	Equipment	Requirements	Qt	Reference Model
		Speaker | Audio in 3.5mm | USB ports x 2 | Picture-by-Picture | VESA 100mm x 100mm | 2y RMA		
4	Servers	Xeon Gold 5520 | 128GB | SSD 1TB | NVIDIA P620 | DVD+RW | 3y RMA	2	Dell Power Edge R740
5	Storage devices (SAN)	2U | Intel Dual core 2.2GHz | Dual Controller 4 x 16Gb FC ports & 4 x 10Gb SFP+ | 4 x 10Gb SFP+ SR | 4x SFP 16Gb FC | 4 x 1x Multi-mode 2m LC-LC FC cable | 16 x 2.4TB SAS HDD 10K rpm 2.5 | 24 x 2.5" drive bays | Up to 276 drives | Up to 3.0PB capacity | Drive support: NLSAS 7.2K 3.5: 4-12TB | 7.2K 2.5 2TB | SAS 10K 2.5: 1.2-2.4TB | SAS 15K 2.5: 0.9TB | SSD: 0.48-1.92TB | SED & non SED FIPS certified | PSU 580W x 2 | 3y 24x7 ProSupport Plus & NBD Onsite Warranty	1	Dell EMC ME4024 Storage Array
6	SAN Switch	24 ports FC16 (16Gb max) & 12 x Module 16Gb SFPs+ | Module Singlemode fiber 1Gb | OM4 LC/LC Fiber Cable, (Optics required) 3m | Aggregate bandwidth: 384Gb full duplex | Rack Mount rails for 4-post Rack | 3y 24x7 ProSupport & NBD Onsite Warranty	1	Connectrix DS6505B 12-24 Port FC16 Switch
7	Switch L3	L3 Switch | 24 x 10/100/1000 Mbps RJ45 PoE+ interfaces | 2 x 1Gb SFP uplinks & 2 x 10Gb SFP+ uplinks | Full duplex switching bandwidth: 160 Gbps | Forwarding rate: 65.5 Mbps | PSU 350W | 512MB DRAM | 128MB flash | 2y RMA	2	3750WS-C3750X-24T-S
8	Switch L2	24 x 10/100/1000 Mbps RJ45 PoE+ interfaces | 4 x 1Gb SFP uplinks | Full duplex switching bandwidth: 216 Gbps | Forwarding rate: 108 Gbps | PSU 250W | 512MB DRAM | 128MB flash | 2y RMA	4	2960X-24TS-L (PORT 1 Gigabit)
9	UPS	Online/Interactive UPS 50KVA | NMC controller | 2y RMA	1	
10	Firewall	1U | 8 x 1Gb RJ45 | 6 x 1Gb SFP | 1Gb RJ45 Mgmt | Console RJ45 | Local Storage SSD (120GB SED) | FW throughput (1500-byte UDP): 2 Gbps | FW throughput (450-byte UDP): 350 Mbps | VPN throughput (IPSec): 300 Mbps | IPS throughput: 650 Mbps | Threat protection throughput: 1100 Mbps |CSC-SSM-20 Plus license & 3DES/AES (license for 2y) | 2y RMA	1	Fortinet FG-80E Fortigate FG-300E Check Point 5200
11	Network Tap	2 x 1Gb RJ45 8 pins | 2 x 10Gb SFP+ | Link Failure Propagation (LFP) | Aggregation/ Regeneration | 802.3af & VoIP compliant | PoE passthrough | Redundant powering | 2y RMA	1	
12	Fortify static code analyzer (or equivalent) for source code review	Software development tools | Integrated Development Environments (IDE): Eclipse, Visual Studio, IntelliJ IDEA | Build Servers: Jenkins, Bamboo, Visual Studio, Gradle, Make | Issue Trackers: Bugzilla, Jira, ALM Octane | Open Source Security Management: Sonatype, Snyk, WhiteSource, BlackDuck | Code Repositories: GitHub, Bitbucket | Swaggerized API for unlimited customization | 1y license	1	
13	Acunetix 360	Acunetix 360 | 3y license	1	
14	Nessus Professional	Nessus Professional | 3y license	1	

ANNEX 12: Activities, Inputs, and Outputs for Each Outcome

Output 1. Capacity of security quality management and policy making is enhanced

Activity	Input	Output	Attachment file
1-1. Clarify the required roles defined in SecBoK framework	JICA Expert	• CDP format • CDP manual (incl. CDP DB, Source Code)	• CDP_FORM-rev08 • CDP manual
1-2. Develop a CDP for each staff based on SecBoK Framework	JICA Expert	• Created CDPs	• CDPs
1-3. Develop a training course plan for high prioritized roles defined in SecBoK Framework (e.g. CISO, Commander)	JICA Expert	• Training list	• Training List, Google Spread Sheet
1-4. Conduct training	JICA Expert local training, raining in Japan	• Training result • Created CDPs • Training materials	• Training Reports • CDPs • Training materials (Japanese Survey result, Marketing theory, Building cyber exercise environment, Malware analysis, GDPR, etc.)
1-5. Review CDP (e.g. every six months)	JICA Expert	• Created CDPs	• CDPs
1-6. Plan and conduct training for policy maker	JICA Expert local training, training in Japan	• Training list • Training result • Created CDPs	• Training List • Summary of Training, Training Reports • CDPs
1-7. Develop/localize awareness raising materials	JICA Expert local procurement	• 3 video material • COP portal site • Branding kit	• Awareness-raising materials

Output 2. Capacity of reactive service is enhanced

Activity	Input	Output	Attachment file
2-1. Develop a training course plan for high prioritized roles defined in SecBoK Framework (e.g. Incident manager, Incident handler, Triage)	JICA Expert	• Training list	• Training List, Google Spread Sheet
2-2. Conduct training	JICA Expert local training, training in Japan	• Training result • Created CDPs	• Summary of Training, Training Reports, Training materials • CDPs
2-3. Review CDP (e.g. every six months)	JICA Expert	• Created CDPs	• CDPs
2-4. Expand reactive infrastructure (e.g. DDoS attack mitigation, malware analysis) in AIS	JICA Expert	• Equipment list	• Equipment List (DDoS Mitigation System) • Equipment List (Malware Analysis)

Output 3. Capacity of proactive service is enhanced

Activity	Input	Output	Attachment file
3-1. Develop a training course plan for high prioritized roles defined in SecBoK Framework (e.g. Researcher, Solution analyst, Vulnerability diagnostic consultant, Information security auditor)	JICA Expert	• Training list	• Training, Google Spread Sheet
3-2. Conduct training	JICA Expert local training, training in Japan	• Training result • Created CDPs • ISAC survey report	• Summary of Training, Training Reports, Training materials • CDPs • ISAC Report
3-3. Review CDP (e.g. every six months)	JICA Expert	• Created CDPs	• CDPs
3-4. Expand proactive infrastructure (e.g. network monitoring, equipment for support practice according to international standard Common Criteria) in AIS	JICA Expert local support	• Equipment list • Lab Security Manual • Security Evaluation Procedure (lightweight) • Security Evaluation Procedure (EAL2+ Common Criteria) • ETR Template	• Equipment List (DDoS Mitigation System) • Equipment List (Security Evaluation) • Lab Security Manual • Security Evaluation Procedure • ETR Template

ANNEX 13: R/D, M/M (copy)

Attached.

ANNEX 14:   Monitoring Sheet (copy)

Attached.

ANNEX 15: Joint Coordination Committee (JCC)

No	Date	Number of participants		Discussion point
		Viet Nam	Japan	
1	24th September 2019	8	9	the project team reported the progress and plans in the future
2	14th August 2020	9	8	the JICA expert and AIS reported the project's activities one year after it was launched and discussed plans for the project. The project, which was originally scheduled to end in November 2021, was extended to March 2022 to include new activities such as security product evaluations, new awareness raising activities, and an information-sharing system.
3	15th September 2021	8	11	both AIS and JICA experts explained the progress and achievements to date and future plans toward the end of the project. In addition, AIS shared the objectives, expected contents, and status of the procedures for the request of the Phase 2 of this project.
4	1st March 2022 (planned)	TBU	TBU	TBU

ANNEX 16: A collection of comments from the CDP review

Question: What did your attitude or way towards work change after you participated in the training?

- **2nd CDP review (A sampling of some specific comments from the 62 responses)**

- ✓ I hope that after the next course I will have a better knowledge base in my daily work.
- ✓ need to arrange time more to spend the time to join the training course be on time.
- ✓ After I have completed the CEH-V10 course, I have knowledge from basic to specialized in security, know how to use the tools and methods of hacker attacks by Modules, then master. attack methods that hackers often use and have the ability to prevent and prevent unauthorized attacks and network sabotage in organizations.
- ✓ I have much more useful knowledge on the field of Information Security and Common Criteria. I feel everything about these fields become clearer and they attract me more to study and work about them.
- ✓ Trainings helps to better manage the team and consult supervisors how to develop cybersecurity.
- ✓ My attitude to work has changed and raised higher for information security.
- ✓ "After I completed the CEH course I applied a lot of knowledge in my work such as: I learned Attack Techniques, Attack Tools and Countermeasures, System Security Assessment and website applications, wireless hacking methods, wireless hacking tools and WiFi security tools, malware analysis and removal, ... Specifically, I participated in training to raise awareness for the provinces. in the southern region, take part in information security drills that the organization trains for the units, ... In addition, I also completed training CISM, I understood the role of each position in the organization, outlined the work goals of each person and the responsibilities of each position of the organization."
- ✓ Although her job is not related to project management much but the PMP course helps her identify which stage of projects her job is. PMP also improves her terminology of project management.
- ✓ It's very useful and helps me to feel more confident to communicate in English.
- ✓ Knowledge studied in trainings help him much in his daily task, for i.e., thanks to CHFI, he could analyze Wireshark package.
- ✓ The courses provide him foundation knowledge of system management. But now his job mainly is related to monitoring so CEH is more useful for his daily tasks.
- ✓ After joining courses, I feel more confident at work.
- ✓ VMware course provides me basic and systematic knowledge on system admin which is useful for my job. I expect that the 2nd VMware course could be more practical and more related to my daily tasks.
- ✓ I learn a lot of practical knowledge through ECSS, CEH and English which are useful for my job, especially CEH course.
- ✓ I gain deeper understanding and practical knowledge on cybersecurity thanks to CEH course. For English course, it helps me to practice pronunciation and communicate with people confidently.
- ✓ better support in the process of pentesting systems, as well as technical troubleshooting
- ✓ Thanks to CAPM course, even I attended just 50% of the training, it helps me to
- ✓ make working plan and manage work better.
- ✓ The CC course is useful for AIS. After the course, we published 2 based standards, 12 criteria and some process to evaluate system.
- ✓ The most helpful and interesting part of the CAPM course is how to make plan (Planning). Because the duration is quite short (5 days) in comparison with big content of the course, so it is not easy to apply all in my daily tasks. But it still helps me somehow in my job.

- ✓ The CompTIA S+ training is useful, which I can utilize in inspection activity.
- ✓ It's helpful for me, but the course duration is not enough to absorb huge knowledge of the CompTIA S+
- ✓ Although I studied the CompTIA S+ by myself but thanks to the course, I discussed with the trainer and find answers for some of my concerns/questions related to my job.
- ✓ The ECSS is a basic course which provides overview of cybersecurity. The knowledge is quite new and useful for my job.
- ✓ The courses are very helpful because they provide exact answers for my questions on what I concern. For English, it helps us to speak, write fluently.
- ✓ Although the PMP course provides only theory, a part of the course (Planning) is still helpful, and I could apply a little into daily jobs.
- ✓ Thanks to the course, I know terminology of cybersecurity and apply English reading skill into my translation job when I collect information to make news.
- ✓ Knowledge and skills provided in the training are important and useful for VNCERT HCMC. However, the course contains huge knowledge and 5 days duration is not enough.
- ✓ ECSS course provides fundamental technical knowledge which is useful for me. I know how to protect my personal computer by using firewall, or be more careful when I open emails, use the Internet.
- ✓ PMP course is useful, which help me to make plan and allocate human resource for each task. CISM provides risk management knowledge which is essentially necessary for VNCERT while we plan to formulate regulations on this content.

- **3rd CDP review**

- ✓ The knowledge in ECSS course has helped me a lot in my working process, from providing more basic knowledge about computers such as OSI network model, TCP/IP network model, network protocols. often used as HTTP, HTTPS, DNS.. to in-depth encryption knowledge like RSA MD5.. knowledge related to safety and network security such as viruses, trojans or network attacks such as XSS, SQL injection.
- ✓ I feel more confident at work
- ✓ It is my daily job to analyze cyber threats to warn. So after taking some courses like CEH. It helped me to be more at the process of a network attack
- ✓ "CISM: the course is useful which provides general view on security management, however, it's difficult to apply methodology or concepts (job title, task...) into Vietnam system because of the difference between international models and Vietnam model.
- ✓ Every course make me understand more and more. We really need the courses like these.
- ✓ The courses help me to understand English terminology
- ✓ LPIC-1: Provide overview of system while I have to work with Linux. English course (Language Link): It helps me to improve English skills. The course is much better than other courses which I have to pay by myself.
- ✓ English course provides basic English which helps me to systematize the language.
- ✓ ECSS course provides general foundation of cybersecurity which could be useful for me.
- ✓ ISO 27000 Family helps me with risk evaluation which could be utilized in my daily job.
- ✓ CAPM helps me to well manage working schedule to improve daily tasks; English course sounds an interesting course in which the trainer knows how to motivate students and provides systematic basic knowledge
- ✓ ISO 27000 Family course which contain practical knowledge is quite useful for my tasks
- ✓ ISO/IEC 17025: Provide templates to evaluate products

- ✓ I feel improvements in my awareness of security, how our information systems can be affected or attacked by internal and external threats, and how we can reduce detrimental outcomes by some basic mesures.
- ✓ ECSS is an useful and practical course which helps me how to protect data by encryption. The duration is short, it is still considered to provide helpful practice. Although the course material is in English, I have to translate every page, and being a non-technician, I still enjoy the course much.
- ✓ CISA is an interesting course for me but because of my workload so I cannot attend the course fully. For CTIA, it provides basic knowledge.
- ✓ Make me feel confident, approach and solve problems faster
- ✓ I have formed a security mindset in my daily work
- ✓ ECSS: provide knowledge on VPN which is helpful when I have to work remotely by knowing and understanding cybersecurity.
- ✓ CTIA: though the course is more difficult than ECSS, it closely links with my daily tasks while I have to collect information. The part of Zero day vulnerability is especially interesting.
- ✓ English: Trainer is good but curriculum is so basic, simple and has not improved my skills.
- ✓ After the course, I used the knowledge combined with the Team to organize training to raise awareness of information security, analyze and remove malicious code. then organize a rehearsal for the training participants. To visualize the incident response process at the agency and the steps to take.