# Transcript

## Section A

00:00:01 Interviewer

Um, now we are going to conduct an interview with TPU6.

00:00:10 Interviewer

Okay, let's start with Part A. For the first question, you belong to a public sector, yes. For the second question, may I ask which unit you work in?

00:00:22 TPU6

I am currently in the [a government criminal investigation unit].

00:00:29 Interviewer

Hmm.

00:00:29 Interviewer

Okay, how long have you been working in this unit?

00:00:32 TPU6

Um, I've only been here for 3 months, but because I was previously in the [a government criminal investigation unit] for about 6 years.

00:00:44 Interviewer

OK.

00:00:45 Interviewer

6 years there and about 3 months here? OK, so your position is Detective, right?

00:00:51 TPU6

Yes, Detective.

00:00:53 Interviewer

And what are your responsibilities?

00:00:54 TPU6

Um, my current job is, I would say, I will do... We have a self-built system in our [the name of a government crime analysis unit] that is responsible for crime analysis. I am now responsible for the management of this system. And in our collaboration, we also have a [the name of a government intelligence unit focused on crime analysis], where my role is more focused on intelligence analysis and system management.

00:01:20 Interviewer

Okay, got it.

## Section B

00:01:23 Interviewer

So, let's move on to Part B. For the first question, based on your understanding, what are the main types of cyberattacks that Taiwan is facing currently? And what are the techniques used in these attacks? Could you give some examples to explain?

00:01:40 TPU6

Actually, for this part, I think it depends on which county or city we are talking about. For example, I used to work in New Taipei City before transferring to Taipei City. The experience was different because there are fewer companies in New Taipei City compared to Taipei City.

00:01:58 Interviewer

Fewer companies?

00:01:59 TPU6

Yes, fewer companies and businesses. Their headquarters are mostly located in Taipei City instead of New Taipei City. After working here for a while, the most common cyberattacks we encounter are data leaks from e-commerce websites, which was rare a few years ago, as well as DDOS attacks and scams involving virtual currencies.

00:02:27 Interviewer

I see.

00:02:27 TPU6

Regarding the techniques used in these attacks, I can give an example of a DDOS case that happened around 2019. There was a teenager who set up a service on the internet, providing several plans for customers to pay for. After paying, the teenager would attack the website designated by the customer.

00:03:01 TPU6

We caught him because he tried to test his DDOS skills by attacking the Investigation Bureau's website.

00:03:13 Interviewer

I see.

00:03:14 TPU6

Later on, at that time, the website of the Investigation Bureau was hacked, and then we became aware of the existence of this person, who was providing a paid service.

00:03:22 TPU6

In the investigation process, because now most people are used to using proxies or VPNs, if we simply use IP, it's basically impossible to trace him in Taiwan, because Taiwan cannot request information from these service providers to give us the information of VPN users. So, based on my practical experience, I would trace his payment flow. If he provides a service, customers will have to pay for it, and during the payment process, the customers may use credit cards or transfers. If he uses this method to receive payments, it will be easier to track him, because inexperienced hackers, who are often high school or university students and lack criminal experience, usually don't set too many breakpoints in payment.

00:04:22 TPU6

So, we can track him through his payment process, trace him to his account, and then locate him in the south...

00:04:33 Interviewer

Locate this teenager?

00:04:33 TPU6

Yes, this teenager.

00:04:39 TPU6

Then, if it is that one, the more common one compared to what I just mentioned is the database leak. I have dealt with the database leak before, and we have divided it into two types. The first type is that there might be an insider within the company who has connections with other vendors or hackers, enabling them to carry out certain activities. The second type is that it could be a general case of data breach where information is leaked. As an example, there was a well-known company called [the name of a Taiwanese company for funeral services] that was involved in life insurance services.

00:05:11 Interviewer

Oh, yes, yes, yes, I see.

00:05:14 TPU6

At that time, they also had a case of data leakage in 2020, and at first, everyone thought that it might have been attacked by hackers. But later we suspected that because... it is not easy for hackers to obtain computer permissions, I think it is relatively difficult to obtain computer permissions now.

00:05:20 Interviewer

Hmm.

00:05:37 TPU6

Because as long as its devices are relatively new, it is difficult to obtain permissions for them.

00:05:43 TPU6

So, in this case, they were able to gain access to the company's database by obtaining the account credentials of a vice manager. It's possible that the vice manager reached some sort of agreement with them or they paid a certain amount. Once they had the account credentials, they could directly invade the company's database and retrieve the data. This breach occurred because they had access to the account, creating a vulnerability. Another possibility is that they used social engineering techniques such as email phishing to gain access to the company's database and cause a data leak.

00:06:23 TPU6

We have solved more cases for these two types. Another method is related to vulnerabilities in VPN access. Some companies use VPNs to access their databases remotely. In some cases, we have discovered that certain maintenance vendors or the VPN itself had vulnerabilities that allowed unauthorized access. This enabled attackers to breach the vendor's system and retrieve data from multiple e-commerce companies that were clients of that particular vendor. That's probably it.

00:06:58 Interviewer

OK, got it.

00:07:00 Interviewer

Okay, let's move on to the second question. What do you think is the main target of cyber attacks in Taiwan currently? And what are the reasons for it? Why has it become a target?

00:07:13 TPU6

As for cyber attacks, I think one of the most common targets is the e-commerce industry, because they have access to their customers' data.

00:07:26 TPU6

With this data, cyber criminals can conduct credit card fraud, scams, or use the personal information to conduct sales or even steal account information to defraud that victim’s friends and family. This allows the criminals to jump through several layers of security.

00:07:51 TPU6

Another reason could be related to Taiwan's political environment. In recent years, any political-related incidents have been targeted by attacks from China due to political reasons.

00:08:04 Interviewer

I see.

00:08:06 Interviewer

Okay, this leads us to the third question. What do you think are the factors that affect internet security and safety in Taiwan right now?

00:08:15 TPU6

I personally think it's more of a problem with the people in Taiwan rather than the devices themselves. Taiwan tends to use advanced software, which are produced by well-known foreign companies, for their devices and software. As long as you have money, you can buy them. However, most people in Taiwan lack basic knowledge of cybersecurity, even though there have been some public awareness campaigns.

00:08:44 TPU6

Many people think that since information is related to technology, they are unwilling to understand its details and processes. As a result, they may overlook these concepts of cybersecurity and end up without even basic knowledge. For example, with computer passwords, we often require people to change their passwords every three months and include uppercase and lowercase letters, numbers, and certain lengths.

00:09:15 TPU6

But as it progresses, because these passwords become too complex and combined with the regulations set by some banks, users might end up writing down these complex passwords on a piece of paper, a notebook, or even on their phone in a certain place.

00:09:32 TPU6

However, there have been advancements in technology, such as using Face ID or biometric authentication. Unfortunately, the legal framework in Taiwan is somewhat outdated, and it hasn't fully embraced biometric authentication as a standard method for banks or certain specialized e-commerce platforms. As a result, relying solely on passwords and two-factor authentication has become vulnerable and susceptible to being compromised over time.

00:10:01 TPU6

This is why people's information is so easily leaked, and I think it's a problem with the general public's knowledge.

00:10:12 Interviewer

So, people's knowledge of information security is not sufficient?

00:10:19 TPU6

It's not sufficient, and it's a bit like having a background in information technology. For example, because most people with an IT background may have studied computer science, and computer science and information management are not the same. Computer science does not teach you how to communicate with the general public. This means that when they try to educate people about information security, they can't explain it in a way that the general public can understand because they are too technical, and people have no idea what they are talking about.

00:10:47 Interviewer

They need to use more understandable language.

00:10:52 TPU6

If they study information management, they may be too focused on management, and what they teach may not be able to integrate with the theories of information security because information management in Taiwan does not include information security. In principle, the study of cybersecurity is mainly in the field of computer science, but computer science students are not typically skilled in communication and marketing.

00:11:19 Interviewer

OK, I see。

00:11:22 Interviewer

Because we talked about politics just now, do you think politics is also a factor?

00:11:29 TPU6

Do you mean this is a factor affecting Taiwan? Yes, because our recent understanding is that Taiwan is different from China. China has systematic regulations related to network management and network attack.

00:11:47 TPU6

Regarding Taiwan's network army, as far as we know, for example, the Coast Guard Administration and the Ministry of National Defense, their network army is more limited. They are mainly responsible for the maintenance of their own facilities and equipment. They may have some red and blue team exercises and attack techniques, but if they don't rely on machines, they don't have much experience in attack and defense. This is why there are more systematic attacks on Taiwan.

00:12:16 Interviewer

I see.

## Section C

00:12:18 Interviewer

OK, then let's move on to the next section. In section C, I'd like to ask the first question about your understanding. What do you think is the overall plan for Taiwan's government on network security? Of course, with regards to these plans, how would you evaluate them?

00:12:41 TPU6

In fact, Taiwan had a department dedicated to cybersecurity planning many years ago, although I don't recall its exact name. This department would outline a cybersecurity roadmap for Taiwan, planning for 5 to 6 years ahead with a white paper detailing the objectives and tasks to be accomplished during this period.

00:13:04 TPU6

That's right. Even though the cybersecurity planning is carried out in stages, many people may not feel its impact in their daily lives or on their assets. The public might have little awareness of how these cybersecurity measures actually protect their personal information and property. However, in terms of passwords, there might be more tangible effects. For example, in the military sector, they still rely on physical codebooks, and without access to these physical documents, it becomes difficult to decipher their passwords. As for encryption algorithms used in other sectors, they are generally similar and follow standard practices. Regarding IoT, Taiwan may be somewhat behind in terms of cybersecurity regulations. Only in the last year or two has the private sector started to take control and form associations to assist in setting standards. However, these regulations do not seem to have significantly impacted government agencies. When companies want to sell IoT products, they only need to comply with the cybersecurity standards. Once they pass the testing in Taiwan and meet the cybersecurity requirements for their IoT devices, they can then sell them overseas. This is the current situation.

00:14:31 Interviewer

OK, so do you think this plan is good enough, or is it inadequate? Or do you think there is a need for improvement?

00:14:46 TPU6

I think the current situation is actually sufficient. However, one area that needs improvement is that they haven't made enough efforts to revise related laws. For instance, starting from last year, they have required companies with certain capital to appoint a Chief Information Security Officer (CISO). But since Taiwan has a shortage of cybersecurity professionals and experienced experts, they can only look for candidates from specific government agencies or those with relevant experience. It's challenging to find suitable candidates because there is a scarcity of talent in this field. I believe one of the main reasons for this shortage is the relatively low salary offered for these positions.

00:15:29 Interviewer

That's the reality.

00:15:29 TPU6

He would rather work in the public sector or find a job that offers slightly higher pay than working outside.

00:15:36 Interviewer

Okay, then we move on to the second question. The second question is about your understanding of the prevention strategies against cyber threats in the public sector. How do you evaluate these strategies?

00:15:54 TPU6

In the public sector, they categorize organizations based on the level of sensitivity of their data. B or C grade. For example, organizations like the household registration (戶政) under the Ministry of the Interior, which handles personal information, may be classified as higher-level. Similarly, the police department might receive a B grade due to their handling of criminal records and personal information. Some sub-offices might receive a C grade if they lack proper data retention and system setup. However, there is a significant flaw in this system. They only require these organizations to allocate around one to three percent of their budget for information security annually. Some local governments restrict this requirement only to municipal governments, fearing that other organizations might not allocate a suitable budget for cybersecurity measures.

00:16:53 TPU6

In this case, the budget allocation is very low, so it is not even enough to purchase equipment. Therefore, in the past one or two years, they have mainly focused on promoting education and training or basic e-mail and social engineering exercises.

00:17:08 Interviewer

I see.

00:17:09 TPU6

Their most successful achievement should be that the vast majority of public sector employees will not click on suspicious e-mails. This should be the most successful aspect.

00:17:19 Interviewer

OK.

00:17:20 Interviewer

So, for the third question, where do you think improvements can be made?

00:17:27 TPU6

Well, if they want to improve the situation, when formulating these policies, they should require that the CISO in these organizations be appointed from the deputy heads of the respective units. However, the reality is that most of these deputy heads lack relevant information security knowledge. Ideally, there should be an information security framework established within the public sector. It seems that the Ministry of Digital Affairs is discussing this, but it has not been implemented yet and is still under consideration.

00:18:01 Interviewer

Understood. Okay, let's move on to the fourth question. Since we were talking about prevention earlier, the fourth question is about what strategies are in place to respond to the underway cyber attacks in the public sector. Do you know if there are any response strategies, and how would you evaluate them?

00:18:22 TPU6

Actually, for the vast majority of the public sector, if it is a department with a special nature, it will turn its own network into a closed one, such as the police or the Ministry of National Defense. It becomes a closed network, but there are still some special external network lines that can be attacked. But if you are just a non-special public agency, they do not have this type of protection, and I think this is mainly due to budget constraints.

00:18:51 TPU6

Because most of the network attacks are based on the vulnerabilities of your system and equipment. Most of the public agencies do not take fixing their server versions and system vulnerabilities seriously. If they want to make improvements, they should find ways to upgrade their servers or systems and repair those technical vulnerabilities.

00:19:14 Interviewer

OK.

00:19:15 Interviewer:

Okay, so for the fifth question, let's continue from the previous question. In which aspect do you think improvements can be made or done better?

00:19:24 TPU6

If they want to improve, the current situation involves some municipal units taking the lead in assisting various agencies with tasks such as source code scanning or vulnerability detection.

00:19:37 TPU6

Source code scanning refers to scanning whether there are vulnerabilities or risks in the program code itself.

00:19:47 TPU6

During such assessments, they will check for any vulnerabilities in your system that could be exploited by attackers. They may also review whether the components used in your systems have been regularly updated. However, the improvement process should include evaluating the performance of the service providers. Although some service providers may be capable of conducting proper evaluations and improvements, others might lack the expertise to assess and address these issues effectively. Instead, they may provide simple reports generated by software and pass them along without much insight or action.

00:20:26 Interviewer:

Oh, okay, got it.

00:20:33 Interviewer:

Now I'll move on to the sixth question, because just now we talked about during the attack. Question two is asking about after a cyber attack, public sector organizations usually have some measures for review and reflection, and they will think about how to respond next time. How would you evaluate these measures?

00:20:54 TPU6

Right, in most cases, the corrective measures would involve instructing the lower-level staff not to engage in certain activities, such as clicking on suspicious links or accessing unfamiliar websites and emails. However, apart from these general improvements, there are no concrete actions taken to address the root causes of the issues. For example, in some cases, if they find a security flaw or deficiency, they can only issue warnings to the individuals responsible and advise them not to repeat the same mistakes. However, there may not be corresponding penalties or consequences for those individuals if they continue to neglect security measures.

00:21:08 Interviewer

Hmm.

00:21:30 TPU6

Even some government agencies do not allocate additional budgets to upgrade their existing hardware and software vulnerabilities. This is because everyone in the government is limited by the complicated process when implementing something. Most people are unwilling to go through the cumbersome process.

00:21:50 Interviewer

Okay, so for the seventh question, do you think the areas for improvement are what you just mentioned?

00:22:01 TPU6

I actually think that if they want to make improvements, they should consider establishing a dedicated agency or department with experienced professionals in each organization. The current situation is that the law requires appointing specialized cybersecurity personnel, but most organizations are large, and having only one person in charge is not sufficient to handle the necessary maintenance and security effectively. Ideally, they should have a small but capable team, instead of just relying on a single individual.

00:22:39 Interviewer

So, generally speaking, is the shortage of cybersecurity talents still an issue?

00:22:42 TPU6

Well, it's not that there is a shortage of cybersecurity talents, but rather that the organization doesn't have the corresponding structure to accommodate these cybersecurity talents.

00:22:52 Interviewer

I see, okay. So now we move on to the eighth question. What do you think about the general public's awareness of cybersecurity nowadays? You mentioned it before.

00:23:04 TPU6

Yes, the awareness is to not casually disclose their passwords to others and to set a more complicated password. Other than that, they don't know anything else.

00:23:15 Interviewer

They don't have any specific awareness, in other words, they don't have a sense of crisis, right?

00:23:22 TPU6

Right, because they may have received a lot of technical propaganda and been told about it, but unless experiences it by themselves, such as his account password or social software being defrauded, people who haven't had these experiences won't be able to understand it deeply.

00:23:38 TPU6

Usually, people who haven't gone through such experiences just can't understand it deeply.

00:23:43 Interviewer

Oh, I see. Usually, it's like that. You have to go through it to know the pain.

00:23:51 Interviewer

Okay, let's move on to the ninth question. As we just talked about, the general public lacks knowledge about cybersecurity. Does the government have any plans to educate the public about cybersecurity? Are there any educational programs available? And how effective do you think these programs are?

00:24:14 TPU6

Well, there are some regular promotional and training courses available, and they may also post some publicly available videos on the Internet. However, the problem is that they cannot provide targeted education based on different levels of knowledge. For example, if you talk to someone who is more experienced about basic knowledge, they may find it boring. On the other hand, if you talk to a beginner about complicated knowledge, they may not understand it. Therefore, the government has not systematically targeted different groups for appropriate promotion.

00:24:50 Interviewer

Okay, so it's like we need to tailor education to meet individual needs?

00:24:55 TPU6

It's not necessarily tailored education, because they don't have a systematic and phased education program. It seems that they only focus on recent occurrences of cybersecurity incidents and provide education based on those specific events that have been happening frequently.

00:25:30 Interviewer

Okay, let's move on to the tenth question. What is the government's current recruitment or training plan for cybersecurity talents in schools and outside of schools? And what do you think of these plans?

00:25:30 TPU6

As I am currently studying in graduate school, I know that the Ministry of Education has set up a cybersecurity talent cultivation plan. They invite cybersecurity professionals to universities to give lectures or to promote digital forensics and cybersecurity forensics, among other things.

00:25:53 TPU6

But his biggest problem as a talented person is that when he wants to find a job, he finds that there are not many good jobs available on the market right now.

00:26:05 Interviewer

Oh, okay.

00:26:07 TPU6

Unless he goes to work abroad, because if he stays in Taiwan, the only jobs available for him are in hardware security, some auditing work for accounting firms, but most of these are still in the learning phase. As for digital forensics companies, there are only one or two, so he doesn't have many options.

00:26:30 TPU6

Therefore, the jobs he will look for more often are IT personnel. He thinks that with his basic IT management knowledge, he can do security work like firewalls and equipment, or related management work. But he only does that because he has a foundation in IT management.

00:26:48 Interviewer

Don't they have any other choices? Okay, okay, so currently in Taiwan, there are relatively few security companies, right?

00:26:58 TPU6

Well, there are actually no companies. For example, a company may post a job opening, and that one job may require you to be in charge of the entire company's security. The salary may only be around 40,000 to 60,000 NTD, which is already considered high.

00:27:17 Interviewer

Okay, okay.

00:27:19 TPU6

There may even be lower paying jobs available.

00:27:20 Interviewer

Oh dear.

00:27:20 Interviewer

So, do different companies set up their own job openings for positions like information security?

00:27:25 TPU6

Yes, positions like information security systems engineer or information security analyst, but this person would have to handle all of the company's information security work.

00:27:34 Interviewer

Wow, that sounds tough.

00:27:38 Interviewer

OK, but for companies that offer services like this for information security, they're relatively rare in Taiwan, right?

00:27:45 TPU6

Yes, they're not exactly rare, but they're considered almost not be seen.

00:27:49 Interviewer

Almost not be seen, OK. So does that mean that there aren't many career options for people with these skills?

00:27:55 TPU6

Yes, there aren't many. Unless you go abroad, for example, to large companies like TSMC or Trend Micro, who actually have information security departments, but the threshold for these departments is very high, as they usually require several years of work experience. I think the most difficult thing to accumulate in information security is work experience, because it's hard to find a suitable company that can allow someone to accumulate experience in this field. Other than working in departments like our police technology crime investigation team, there are few opportunities outside to accumulate this kind of experience.

## Section D

00:28:35 Interviewer

Okay, let's move on to the section D. The first question I want to ask is, what do you think about the concept of collaboration between the public and private sectors in the field of cybersecurity? Does it really contribute to the development of cybersecurity?

00:28:57 TPU6

Um, I think this might be related to the nature of the public sector. When public and private sectors collaborate, most of the cooperation is driven by interests. If a private company cooperates with the government, it may gain some contracts or business opportunities. However, in return, the government officials might not receive any kickbacks or benefits, and this can raise concerns. Although the direction of cooperation is good, in the current situation in Taiwan, it's unlikely that government officials have ambitious ideals and are incorruptible. So, in most cases, issues related to interests and regulations concerning government officials can lead to many subsequent problems, in my opinion.

00:29:51 Interviewer

Do you think it's difficult to implement this?

00:29:54 TPU6

Implementing this is not easy because you are likely to encounter people questioning whether there are any conflicts of interest between you and them.

00:30:05 Interviewer

Okay, but overall, do you think it is necessary for the public and private sectors to collaborate?

00:30:14 TPU6

I think if they follow a standard bidding process, for example, where we are not engaging in exclusive cooperation, it would be more reasonable. In some cases, they may hire consulting services from external vendors. For instance, the Prosecutor's Office, although they have legal expertise, they may have some prosecutors who have information experience, but they may not have much knowledge of cybersecurity. Therefore, they outsource to cybersecurity firms to provide advice and assistance in their cases and judgments.

00:30:50 Interviewer

I see, OK.

00:30:53 Interviewer

Okay, let's move on to the second question. So overall, regarding internet security, do you know if there are any public-private sector collaboration models, experiences, or examples in Taiwan?

00:31:08 TPU6

Ah, I see. In the past, there was a foundation related to information, probably the Institute for Information Industry (III), and the Criminal Investigation Bureau (CIB) sought their assistance in cases of data breaches in e-commerce. III would then hire consultants, often from external companies, to provide guidance and support to those involved.

00:31:29 Interviewer

I see.

00:31:42 Interviewer

Okay, so these collaborations, well, based on what you just said, these collaborations are not yet mature, right?

00:31:52 TPU6

There is no established system for these collaborations. It seems that the cooperation is more based on the relationships between the current personnel and the relevant departments. They assist when they are familiar with the agency or organization involved, but if there are changes in personnel or new staff members take over, they may not continue to maintain contact or provide assistance.

00:32:13 Interviewer

Okay, good. So for the third question, how do you evaluate this collaboration model, given that there isn't a set mechanism for it?

00:32:27 TPU6

Well, how to evaluate it? I think it comes down to establishing some basic standard operating procedures. For example, when they need to collaborate, they should notify which vendors and departments will be involved and specify the kind of assistance required from these departments. I believe they should make these procedures more concrete and well-defined. Currently, everything seems to rely on informal discussions, saying, "Let's talk about it later" or "I'll explain it to you later," but that "later" may never come.

00:32:58 Interviewer

Hahaha.

00:33:01 Interviewer

Okay, then you've also answered the fourth question, because, actually, questions three and four can be answered together, right?

00:33:07 Interviewer

Alright, then let's just jump to the fifth question. The fifth question is whether your current unit has any experience in collaborating with the public or private sector in terms of network security?

00:33:19 TPU6

Well, in my current unit, let me share my previous experience. In the past, I worked in another unit for a longer period. Around the year 107 (2018), when there were no devices to crack iPhone phones in Taiwan, we went online to Google some news to find out which company could crack iPhone devices. At that time, there were no authorized agents in Taiwan. However, because I had connections with a software company based in Canada, we were able to directly contact their business in Canada. They helped us establish contact with the mobile phone cracking company and arranged an introduction, which eventually allowed us to bring their device to Taiwan.

00:34:21 Interviewer

Okay, got it.

00:34:23 Interviewer

As for the sixth question, how would you evaluate this kind of collaboration mechanism? Is it good or bad?

00:34:30 TPU6

I think this actually places a significant risk burden on the relevant handlers and users, and there is a fear of being accused of favoring a certain vendor or company.

00:34:44 Interviewer

Hmm, OK, so in which area do you think we can improve to make our collaboration better?

00:34:55 TPU6

I think this should be handled proactively by general county or city governments, or even central agencies, to coordinate and resolve these issues. In the past, when procuring software, each region used to allocate its own budget, and it depended on whether the county or city government had sufficient funds. However, starting from this year, there's a new approach where the central government centrally allocates the budget for the entire country and then distributes it to different regions. This centralized method is better than the previous one where each region had to allocate its own budget, which I believe was not ideal.

00:35:35 Interviewer

Oh, so there should be a central government to push and lead, and there will be a unified system and process?

00:35:42 TPU6

A unified system and process, well, it only started at the end of last year, so this year is the first year of its implementation. It might encounter issues because the contracts were signed for three years, and after those three years, it's uncertain whether there will be a budget allocation. If, after three years, the central government stops centralizing the budget allocation and tells each county and city to prepare their own budgets, it could disrupt the funding for these equipment purchases, and the authorization may not be obtained again.

00:36:17 Interviewer

OK, what I just mentioned is that there is a three-year contract signed between whom and whom?

00:36:25 TPU6

Oh, it means that the central government makes a single three-year contract with the vendors for procurement.

00:36:31 Interviewer

OK, got it.

00:36:33 Interviewer

So, actually, most of the improvements are in terms of the system, and there should be people in power to promote it?

00:36:46 TPU6

In Taiwan, the political culture is such that the regular executing agencies generally cannot independently decide on the direction and approach they want to take. They must align with the ideas and decisions of higher-level authorities, such as the Executive Yuan or the President, before they can implement any plans. Moreover, they should avoid deviating too much from those higher-level guidelines.

00:37:09 Interviewer

Haha.

00:37:16 TPU6

If you deviate too much, you may be questioned or challenged.

00:37:18 Interviewer

OK.

00:37:22 Interviewer

Great, thank you. That's about it.