

**RESPONSE BY SECOND MINISTER FOR HOME AFFAIRS TO THE MOTION  
OF ADJOURNMENT ON SECURITY LAPSES – PARLIAMENT SITTING ON  
MON, 21 JUL 2008**

- When a security lapse occurs, it is natural to ask what and why it happened and what do we do going forward to avoid future lapses. These appear to be straight-forward questions. But the answers cannot and should not be simplistic.

What & why it happened?

- I need not go into detail about the recent three cases. Ms Rajah and Dr Teo have pointed out that the common thread running through them was a failure to comply with SOPs. We acknowledge that.
- However, in considering these lapses, we should not oversimplify the issues. If we look at the three cases within their operating context, we can see that one type of mistake is not the same as another, even if the common thread is persons failing to comply with SOPs.
- For example, in the passport misclearance case, the officer's focus was on security. He rightly conducted a face-to-face clearance when the automated gates failed. Terrorists are known to use real passports and in their own identities. Thus such an assessment is important in our counter terrorism security clearance system.
- The officer in question is quite experienced. He assessed Mr Ang by examining, if Mr Ang fit a terrorist or security-risk profile; whether he exhibited any suspicious behaviour cues or indicators; whether the passport tendered was tampered or a forgery.
- Up to that point, the officer did everything right. The officer however made a mistake in not pursuing Mr Ang's failure to clear the automated gates. He was satisfied that Mr Ang was not a security risk, and assumed that it was just a technical glitch. He will be penalised for that error. But we must also be fair to the officer in question. He exercised most of the security protocols correctly, but made an error in not checking the passport against the boarding pass. To equate this case as the same as that of the Mas Selamat escape would be quite wrong.
- Why is this distinction important? I make it not to excuse any mistake or to trivialise one over another. But we need to highlight it because such a distinction is built into the design of all risk-based security systems.
- Security systems are designed to minimise not just failure but also to mitigate the magnitude of specific failures. This is inherent in any risk-based approach

to security. We have to prioritise our resources and focus according to the risks. More resources are focused on high risk, high-consequence areas and less resources in lower-risk, lower-consequence areas.

- Will there be a misclearance case in future? More than 140 million travellers pass through our checkpoints annually. Five cases of persons carrying the wrong passports are detected every day by ICA officers. Can we guarantee that we will pick up all of these and that there will never be one which we might miss? While the Home Team will certainly work to avoid such an instance, it would be fool-hardy and unrealistic to assume this. What we can assure you is that we constantly work to minimise such lapses because we take them seriously. What we can assure you also is that the security system is layered and robust and is structured to minimise serious consequences.

#### What should be done going forward?

- We will certainly review lapses and seek to learn from them. We are doing so.
- Officers who make mistakes or who are liable must be taken to task. But we must also not over-react and be unfair to the officers. We have to ensure that in our judgement there will be fairness, a sense of proportion and justice, and adherence to established due processes.
- Dr Teo has spoken about the need for more discipline and more audits and more checks. Ms Rajah has made similar points. The question perhaps is really how much more is enough. We do regularly conduct audits and checks and they are important and useful. But these audits cannot prevent episodic individual failure to comply with established procedures. In respect of the lapses which have occurred, the systems and processes were found to be sound.
- So more checks and more compliance audits may not be the total solution. What we have done in MHA is to develop and implement a programme to test operational effectiveness. Since Jan 2007, there is in place a Red Teaming programme with the help of expert external consultants. This programme is designed to evaluate the actual level of competencies, alertness and vigilance of front-line security forces. Such tests help us identify operational blind-spots, weaknesses and the level and quality of vigilance of the front-line officer. The results allow us to then develop appropriate and practical interventions including special training for our front-line officers and their supervisors.
- But even such tests cannot stop the individual officer opening a gate without looking at his screen, nor can it help to prevent an officer failing to check the passport against the boarding pass. These as stated earlier are individual episodic lapses. They are not systemic practices.

## Strict Compliance or Active Empowerment?

- I agree with Dr Teo Ho Pin and Ms Rajah that ground commanders and supervisors have a responsibility to ensure compliance by frontline officers with established procedures. However, in doing so, we want to also ensure that we do not dis-empower our front-line officers.
- Systems and SOPs are inherently dated. They are designed based on known experiences and scenarios. Just as we learn and improve, our adversaries, be they terrorists or criminals, learn and improve all the time as well. Ultimately when confronted with something new, we depend on the front line officer to meet such a challenge through his experience, judgement and initiative. How can we do this? One practical approach we have taken is to invest heavily on scenario-based, hands-on, front-liner training at the Home Team Academy. We want our officers to internalise knowledge and understand their SOPs rather than just comply blindly. We want them to develop good situational awareness and to cultivate good reflexes and instincts.

## There is no 100% Security

- The reality is that no system can be completely fail-proof, either now or in the future. The aim must be to minimise failures and maximise success but also recognise that there will be failures and no absolute 100% success.
- For example, we have a zero tolerance philosophy for drug abuse and death penalties for drug trafficking. Our drug abuse and trafficking numbers are low but not zero. That does not mean CNB has failed or that our policy has failed.
- In 2007, ICA cleared some 143 million travellers through our land, sea and air checkpoints; or close to 400,000 travellers each day. With stepped-up security measures, ICA detected 37,800 cases of smuggling at the borders and more than 2,200 foreigners who attempted to enter Singapore fraudulently. Yet, we know that despite ICA's best efforts, there will be some illegal immigrants and contraband smuggled into Singapore. To expect otherwise is completely unrealistic.
- So when Mr Siew Kum Hong made his points, I think he's got to bear these perspectives in mind and not take all three cases together and lump them together and then say therefore there is a serious situation.
- Perfection is the ideal to aim for. But imperfection is the reality we have to work with each day. We face security challenges with incomplete, elliptical information of the evolving threat. Even so, we must act and make the best

judgement we can. Our officers must not be made to become risk-averse and avoid making judgements for fear of being wrong.

### Is the Home Team over-stretched?

- Question has been raised if the Home Team is over-stretched. The core functions of the Home Team have not changed. But its volume and scope of work have greatly expanded, with increased population, tourist arrivals and more international events which require higher security coverage.
- We have a smaller Police force per 100,000 population when compared to Hong Kong and New York. But our crime rate per 100,000 population is lower than Hong Kong's and three and a half times less than New York City's.
- The new security landscape post-911 has raised significant demands on the Home Team. Unlike in the past, Singapore is today a target for terrorist groups.
- A fundamental question which MHA is exploring is whether we can continue to operate with the current level of resources. Our Home Team officers at the front-line are stretched and strained over a high alert that started since end 2001. The total number of overtime hours ICA ground officers at the checkpoints have to put in every month to cope with the volume of work varies between 23,000 to 28,000 OT hours.
- To consider the impact of this, the Ministry has directed that a human factor study be conducted. The study will look at issues of operational fatigue within the Home Team. The study will also look at resource and manning levels and see if there are sub-optimal areas which need urgent attention.

### Look at Security in Perspective

- Security must always be viewed in its context. For instance, the Subordinate Courts is a place which the public must have free access given its critical function in the justice system. Any Police lock-up facility within the premises cannot undermine or compromise this function. We can enhance the lock-up security there. But it cannot be at the same level as Changi Prison.
- On the ground, security needs to find a balance between efficiency and expediency on the one hand, and effectiveness of security measures on the other. As much as we should maintain our security levels at our checkpoints, we also need to facilitate tourism, trade and social activities across borders.
- We need to look at security as always operating in a context where there are competing imperatives of economic, political and social interests. This is not a bad thing. Indeed a completely security-sealed country is one which will

suffocate enterprise and liberty. It is a cure worse than the disease it is trying to prevent.

- We need therefore to understand that security is not an absolute end. It is always achieved at a trade-off. And risks are always relative, to be managed, and not something we can eradicate completely in any human system operating in a living society. If we over simplify a complex subject like security design and operations, we may create unrealistic expectations of these systems and of the people who will man them. In the end, we only fool ourselves.
- The mistakes which have occurred recently cannot be dismissed. We should confront our mistakes, take ownership and take proper action to deal with them. But let us do so always with a sense of balance and on an informed basis, understanding the context and the complexity of the issues involved.
- Let me assure members of the House that the officers of the Home Team are committed to their work and mission and view the lapses which have occurred seriously. No one is more critical of these lapses than the officers and everyone at Home Team.
- Ultimately, we need to look at the generalised outcome of security in terms of the quality of life we have today. The real test of security must be whether there is a sense of safety, whether people can walk about freely and without fear that they would be robbed or assaulted and whether our police force is trusted, and generally free of corruption and nexus with the underworld. On the score-card whether for crime, drugs or terrorism or for neutralising hazards or even in rehabilitating prisoners to give them a second chance, any objective and honest assessment will conclude that the officers of the Home Team have done a good job compared to their counterparts in other parts of the world, despite the difficult operating environment they face everyday.